ВСТУП

Актуальність дослідження. Технологія – блокчейн і ринок криптовалюти демонструють динамічний розвиток і привертають пильну увагу. Нововведення цієї технології полягає в тому, що інформація про транзакції більш не зберігається в централізованій базі даних, а передається на комп'ютери всіх учасників мережі, які зберігають дані локально. Першим додатком на базі технології блокчейн став біткоїн для однойменної криптовалюти. В останні роки він послужив основою для створення інших блокчейн-додатків, більшість з яких в даний час розробляються у фінансовій сфері.

Фактично технологія блокчейн є універсальним способом зберігання і обробки інформації практично в будь-якій сфері діяльності. Вперше технологію блокчейн описала дослідницька група в 1991 р, розглядаючи її основне завдання як зберігання інформації в цифровому форматі, виключаючи можливість підробки даних. Блокчейн – це розподілена база даних, що містить дані про всі транзакції, які були проведені учасниками системи. Інформація зберігається у вигляді «ланцюжка блоків», в кожному з яких записано певну кількість комунікацій [1]. Будь-яка транзакція в блокчейні – це інформація, яка перевіряється згодом незалежними учасниками і вбудована в глобальну історію транзакцій. У цій технології є набір механізмів, який допомагає системі залишатися незалежною і прозорою. За блоками транзакцій можливо відстежити вірність кожної угоди. Це децентралізована база даних, яка дозволяє виробляти транзакцію анонімно, миттєво і без участі спеціалізованих посередників [2].

Усі транзакції по рахунку відкриті в блокчейні для будь-кого, і кожна відбивається у вигляді комбінації символів із зазначенням угоди, її суми, одержувача та відправника, а також міток часу. Блокчейн є технологією, що дозволяє проводити транзакції між рівноправними учасниками єдиної мережі (P2P-мережі), при цьому відсутня необхідність стороннього посередника, транзакція здійснюється безпосередньо між учасниками мережі. Інформація про такі транзакції не зберігається в централізованій базі даних. Вона передається на комп'ютери всіх учасників мережі, де дані зберігаються локально.

По суті блокчейн – особливий цифровий контракт, за допомогою якого конкретна особа безпосередньо здійснює транзакцію з іншою особою і виставляє їй рахунок. У цьому випадку інформація про транзакції зберігається в комп'ютерній мережі, яка включає в себе комп'ютер покупця і постачальника, що здійснюють транзакцію, в тому числі комп'ютери інших учасників мережі. Банк, як традиційний посередник угод, для даної моделі не потрібен, свідками кожної транзакції між постачальником і покупцем виступають інші учасники мережі, які в змозі підтвердити деталі транзакції,

оскільки вся інформація зберігається локально на комп'ютерах усіх учасників.

Розвиток технології блокчейн глобальний, регулярно з'являються нові стартапи, що охоплюють найрізноманітніші сфери. Головна причина, чому ця технологія випереджає попередні проривні технології і так швидко набирає критичну масу, полягає в тому, що вона з'явилася в епоху цифрової трансформації, яка торкнулася більшості секторів економіки. Вже очевидно, що бізнес і державні структури не можуть ігнорувати потенціал блокчейна, а технологічними компаніями вже практично сформована цифрова інфраструктура, яка необхідна для реалізації цієї концепції. Можливості застосування технології блокчейн в бізнесі і промисловості не знають кордонів.

Проривний характер становить загрозу компаніям, які надають технологічні послуги в різних галузях економіки, таких як фінансовий сектор, енергетика, охорона здоров'я, сільське господарство. Блокчейн сприяє переходу на нові бізнес-моделі і оптимізує бізнес-процеси [3]. Наприклад, фірми, що надають фінансові послуги, при переході на цю технологію для підвищення достовірності фінансових транзакцій і зниження витрат, підштовхнуть діючих провайдерів до впровадження платформ і рішень на основі блокчейн. Однак якщо провайдери упустять цю можливість і вчасно не імплементують технологію, цим скористаються численні блокчейн-стартапи. За таким сценарієм події розвиватимуться в інших областях.

З цією технологією пов'язаний ще один фактор, здатний підірвати бізнес технологічних компаній: прискорення переходу від моделі ціноутворення за одиницю продукту до моделі ціноутворення за фактом проведення транзакції або за фактом використання. Такий перехід вплине на обов'язки технологічних компаній зі сплати податків і дотримання законодавства: скоротить витрати компаній на підготовку податкової звітності, скоротить кількість фактів відхилення від сплати податків, надасть громадськості великий доступ до інформації про компанії і зробить непотрібним ряд професій або, як мінімум, вплине на їх перетворення [4].

На сучасному етапі вкрай важливо керівникам компаній проаналізувати вплив блокчейна на свою організацію, з огляду на його можливість змінювати моделі і процеси, архітектуру продуктів і послуг, і навіть обов'язки по оплаті податків.

Враховуючи вищевикладене тема дипломної роботи є актуальною.

Об’єкт та предмет дослідження. Об’єктом роботи виступають новітні технології систем криптографії та технології blockchain.

Предметом є процес удосконалення сучасних систем документообігу та документообміну на приватних підприємствах за допомогою криптографії та технології blockchain.

Мета та завдання. Метою роботи виступає удосконалення сучасних систем документообігу та документообміну на приватних підприємствах за допомогою криптографії та технології blockchain.

Для досягнення поставленої мети у роботі необхідно виконати низку завдань:

- розкрити теоретичні аспекти сучасних систем документообігу та документообміну на приватних підприємствах;
- провести аналіз сучасних засобів криптографії та технологіїї blockchain;
- описати систему документообігу та документообміну на приватних підприємствах;
- дослідити сучасний стан ринку для криптовалют;
- визначити методичні аспекти проектування системи документообігу та документообміну на приватному підприємсті за допомогою криптографії та технологіїї blockchain;
- розробити алгоритм реалізації системи документообігу та документообміну за допомогою криптографії та технологіїї blockchain;
- навести математичний аспект дослідження;
- запропонувати архітектурУ системи документообігу та документообміну за допомогою криптографії та технологіїї blockchain;
- здійснити практичнУ реалізацію системи документообігу та документообміну на приватному підприємсті за допомогою криптографії та технологіїї blockchain;
- описати структуру системи документообігу та документообміну за допомогою криптографії та технологіїї blockchain;
- здійснити тестування системи документообігу та документообміну за допомогою криптографії та технологіїї blockchain.

Методика дослідження. Структура і логіка дослідження підпорядковані рішенню поставлених завдань. При вирішенні конкретних завдань використовувалися методи логічного, функціонального та системного аналізу із застосуванням економіко-математичного апарату, статистичні методи.

Наукова новизна результатів роботи полягає в наступному:

- уперше запропоновано комплексне рішення удосконалення сучасних систем документообігу та документообміну на приватних підприємствах за допомогою криптографії та технології blockchain;
- наведено методи аналізу середовища сучасних систем документообігу та документообміну на приватних підприємствах: формування хронологічної послідовності типових

впливів базових факторів середовища для їх подальшого аналізу й прогнозу за допомогою криптографії та технології blockchain;

– дістало подальшого розвитку вивчення та розробка методів удосконалення сучасних систем документообігу та документообміну на приватних підприємствах за допомогою криптографії та технології blockchain.

Практична значущість дослідження. Отримані результати можуть бути використані у межах організацій для впровадження засобів інформаційної безпеки по етапах.

Апробація результатів роботи

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ СУЧАСНИХ СИСТЕМ ДОКУМЕНТООБІГУ ТА ДОКУМЕНТООБМІНУ НА ПРИВАТНИХ ПІДПРИЄМСТВАХ

1.1 Аналіз сучасних засобів криптографії та технологіїї blockchain

Існує два визначення терміна Блокчейн (Blockchain):

- розподілена база даних;
- безперервний послідовний ланцюжок блоків, що містять інформацію.

Обидва визначення вірні у своїй суті, але не дають відповіді на питання про те, що ж це таке. Для кращого розуміння технології необхідно згадати, які архітектури комп'ютерних мереж існують і яка з них домінує на сучасному ринку IT-систем.

Всього існує два типи архітектур:

Клієнт-серверна мережа;

Тимчасова (пірінгова) мережа.

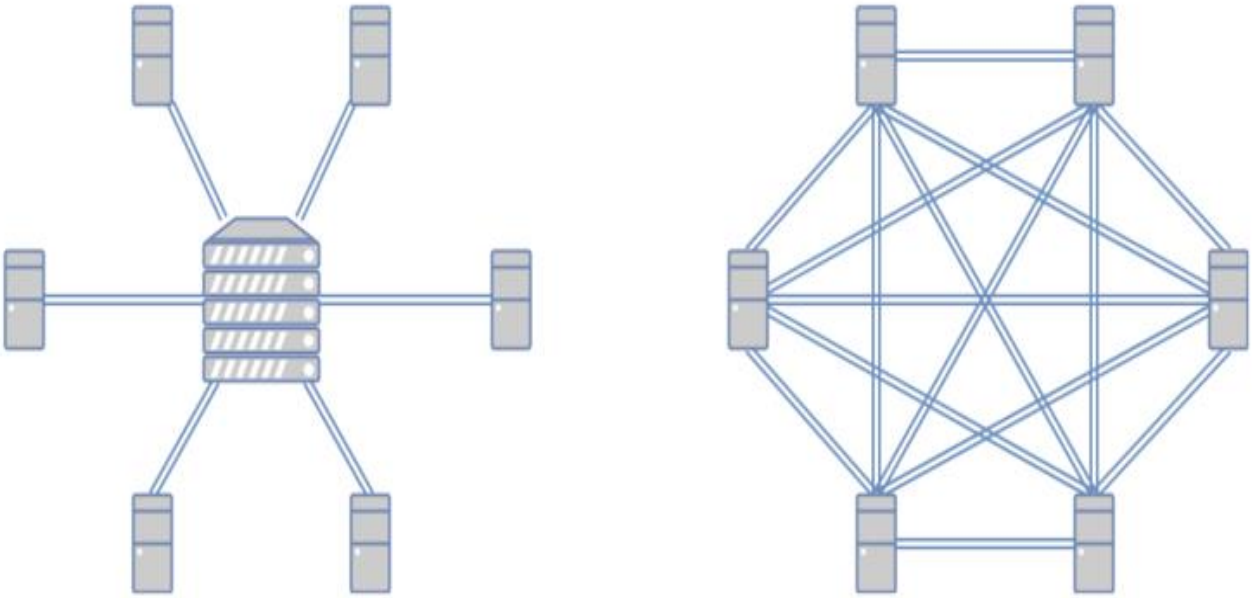


Рисунок 1.1 – Типи архітектур мережі

Організація мережі першим способом має на увазі централізований контроль за всім: додатки, дані, доступ. Вся системна логіка і інформація приховані всередині сервера, що дозволяє знизити вимоги до продуктивності клієнтських пристроїв і забезпечити високу швидкість обробки даних. Саме цей метод набув найбільшого поширення в наші дні.

Однорангові або децентралізовані мережі не мають головного пристрою, і всі учасники мають рівні права. У такій моделі кожен користувач є не тільки споживачем, але і сам стає постачальником сервісу.

Ранньою версією тимчасових мереж є система розподіленого обміну повідомленнями USENET, Розроблена в 1979 році. Наступні два десятиліття були відзначені створенням P2P (Peer-to-Peer) - додатків в абсолютно різних сферах. Одні з найвідоміших прикладів – сервіс Napster – колись популярна файлообмінна пірінгова мережа або BOINC – програмна платформа для організації розподілених обчислень, а також BitTorrent протокол, який є основою сучасних торрент-клієнтів.

Системи на основі децентралізованих мереж продовжують існувати, але помітно програють клієнт-серверним в поширеності і відповідно потребам споживачів.

Переважна більшість додатків і систем для нормальної роботи вимагає можливості оперувати набором даних. Способів організації подібної роботи безліч і один з них використовує метод тимчасових мереж. Розподілені, або паралельні, бази даних відрізняються тим, що інформація в частковому або повному складі зберігається на кожному пристрої мережі.

Одним з переваг такої системи є доступність даних: немає єдиної точки відмови, як у випадку з базою даних, розташованої на одному сервері. Таке рішення також пов'язане з певними обмеженнями по швидкості оновлення даних і поширення їх серед учасників мережі. Подібна система не витримає навантаження від мільйонів користувачів, які постійно публікують нову інформацію.

Технологія блокчейн передбачає використання розподіленої бази даних блоків, які представляють собою зв'язний список (кожен наступний блок містить ідентифікатор попереднього). Кожен учасник мережі зберігає у себе копію всіх операцій, здійснених за весь час. Подібне було б неможливо без певних нововведень, покликаних забезпечити безпеку і працездатність мережі. Це підводить до останнього «стовпа» блокчейна – криптографії.

Шифропанк (Cypherpunks)

В кінці 20 століття зародилося співтовариство, зацікавлене в розвитку анонімності і безпеки в мережі через розробку нових криптографічних методів. Вони вважали, що єдиний спосіб зберегти приватність в мережі – це шифрування даних. перші спроби шифропанків розробити цифрову валюту відносяться до самого початку 2000-них.

Перша версія цифрової валюти була створена Вей Дай і отримала назву b-money. Наступною спробою став Bit Gold, розроблений Ніком Сабо. Обидві валюти володіли великим недоліком – недосконалістю системи прийняття рішення серед віддалених абонентів.

Датою народження повноцінної криптовалюти – Bitcoin, вважається 2008 рік. Саме тоді Сатоши Накамото, зібравши воєдино напрацювання однодумців, виклав у відкритий доступ наукову роботу з описом основних елементів блокчейна, принципів роботи та математичної моделі мережі. Автор з самого початку підкреслює мету роботи – створення нового способу незворотної передачі коштів (транзакцій) між людьми без посередників.

Технологія «Блокчейн»

У перекладі з англійської «Block» - означає блоки, а «chain» перекладається як «ланцюжок». З чого випливає, що блокчейн – це ланцюжок блоків, причому ланцюжок, в якому присутня сувора послідовність.

Тепер про кожну частину детальніше. Блоки – це інформація, дані про транзакції, угоди і контакти всередині системи, які представлені в криптографічній формі. Всі ці блоки збудовані в ланцюжок, тобто мають зв'язок між собою. Щоб записати новий блок, потрібно послідовне зчитування даних з усіх попередніх.

Всю зібрану інформацію неможливо видалити, замінити або підмінити. Дані накопичуються і з них формується доповнювана база.

Головна особливість блокчейн – децентралізація. Немає ніякого основного сервера, на якому тримається вся інформація. Даними володіють одночасно всі учасники блокчейн-мережі. Тобто абсолютно в усіх учасників рівні права, тому здійснення операцій проводиться між ними безпосередньо.

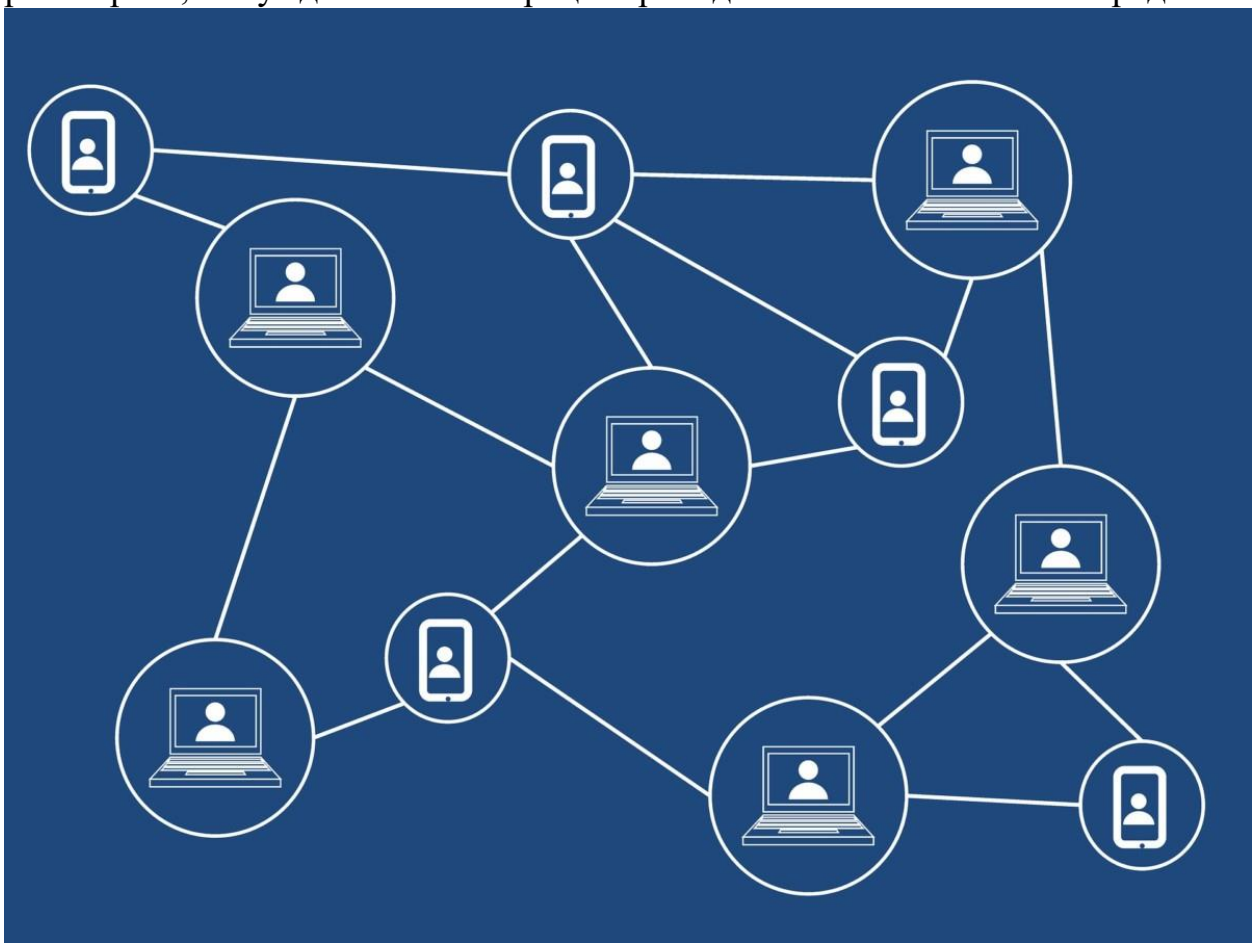


Рисунок 1.2 – Технологія блокчейн – децентралізація

Спочатку технологія була розроблена одночасно з появою біткоїнів, в 2009 році. Творцем блокчейна і криптовалюти прийнято вважати Сатоши Накамото, особистість якого встигла стати міфом. Невідомо скільки людей ховається за маскою Накамото, але очевидним фактом є те, що створення такої технології вимагало одного тижня старанної роботи.

Blockchain ділиться на два основних типи:

1. Публічний – відкрита база даних, яка стабільно доповнюється. Яскравий приклад – віртуальна валюта Bitcoin, де будь-який учасник має право займатися записом і зчитуванням даних.

2. Приватний (також відомий як приватний) – для нього характерні обмеження, що стосуються запису і читання інформації. У ньому деякі вузли можуть мати вищий пріоритет.

3. Ексклюзивний – підвид приватного блокчейна. Особливість його в тому, що обробкою транзакцій в такому ланцюжку займається певна група осіб.

Ключові характеристики і особливості технології:

- Децентралізація. Ні одного сервера, всі учасники є серверами, які підтримують роботу всього blockchain.
- Прозорість. Дані знаходяться в публічному доступі, а їх видалення або зміна виключено.
- Необмеженість. [В теорії] новими ланцюжками блокчейн можна доповнювати до нескінченності.
- Надійність. Необхідність перевірки операції учасниками системи дає можливість «пропускати» тільки легітимні транзакції.

Основний принцип роботи блокчейн

Спробуємо пояснити принцип роботи технології, взявши для прикладу грошову транзакцію:

1. Уявімо, що учасник 1 хоче перевести гроші учаснику 2
2. Транзакції передаються в мережу і формуються в «блоки». Важливо, що кожен блок має номер і хеш попереднього «блоку».
3. Далі всі ці «блоки» розсилаються учасникам системи для перевірки.
4. У разі, якщо помилки відсутні, кожен учасник записує «блок» в свій екземпляр бази даних
5. Після цього «блок» вже може бути доданий до ланцюжку «блоків», що містить інформацію про всі попередні транзакції
6. Гроші від учасника 1 надходять до учасника 2

Формування і закриття блоків

Це один з головних технічних аспектів технології. У кожній ланці ланцюжка зберігається ключ, і закрита ланка можна буде тільки тоді, коли цей ключ розшифрують.

Наприклад в цифрових валютах для розшифровки використовується Майнінг. Для того, щоб добувати віртуальну валюту манери використовують потужності процесорів і відеокарт, які здійснюють певні обчислювальні операції, щоб підібрати криптографічний підпис до «блоку». Тільки після того, як цей підпис буде підібрано, блок зможе закритися, а майнер, в свою чергу, буде винагороджений цифровою валютою.

Ноди або вузли – це особи-учасники блокчейна (в тому числі і Майнер). Саме вони забезпечують стабільну роботу і безпеку blockchain.

Серед них можна виділити повні Ноди – це ті учасники, на пристрої яких міститься повна версія блокчейна. Зараз кількість таких учасників поступово зменшується, що пов'язано із зростанням обсягу блокчейна. Наприклад, обсяг повного блокчейна біткоіни в 2015 році становив 35 гігабайт, а через 2 роки – понад 100.

Варто зазначити, що кількість повних нод грає важливу роль в швидкості обробки транзакційних даних. Більше повних нод – вище швидкість.

Застосування блокчейн за сферами

Криптовалюта. Блокчейн з'явився разом з біткоїн, тому логічно, що технологія використовується у величезній кількості нових віртуальних валют, число яких з кожним днем все зростає.

Внутрішня комунікація. Наприклад, в PayPal почали використовувати блокчейн у власній внутрішній платформі. Співробітникам компанії нараховуються токени за хорошу роботу. Працівник надалі може обміняти отримані токени на якусь із активностей разом з топ-керівниками PayPal.

Вибори. Штат Західна Вірджинія в США став першопрохідцем в такому використанні технології. 140 виборців, які перебували за межами Сполучених Штатів, отримали можливість проголосувати за допомогою блокчейн-платформи, яка була доступна в 22 округах з 44. Експериментальна платформа об'єднувала в собі можливості розпізнавання осіб і blockchain.

Банківська сфера. До слова, саме в цій області на технологію blockchain робляться величезні ставки. Оскільки її впровадження в банківські послуги може прискорити проведення транзакцій, а також посилити їх безпеку. Банки вже почали потроху використовувати технологію в абсолютно різних аспектах:

Кредити. В Іспанії першими зважилися на такий крок. Іспанським банком BBVA був використаний приватний блокчейн для того, щоб вести переговори і завершити процедуру видачі кредиту. В кінці операції реєстрація договору відбулася на платформі Blockchain Ethereum.

Альтернативна фінансова і банківська інфраструктура. Papersoft Africa, iVEDiX і група банкірів планують спільними зусиллями запустити рішення на основі технології блокчейн, яке дозволить африканським підприємцям і окремим особам отримати кращий доступ до банківських послуг. У перспективі, це рішення допоможе мільйонам африканських підприємців і окремим особам отримати кращий доступ до банківських послуг, за рахунок можливості доступу до електронних грошей і електронного банкінгу будь-якій людині зі смартфоном.

Боротьба з небанківськими конкурентами. Фінансовий холдинг JPMorgan створив власну міжбанківську інформаційну мережу (IIN), побудовану на базі технології блокчейн. Крім, власне, боротьби з небанківськими конкурентами, IIN дозволяє зменшити затримки в транскордонних платежах. На сьогодні до мережі приєдналося більше сотні банків.

Обробка готівки. Bank of America збирається запатентувати систему, засновану на блокчейн-технології, покликану поліпшити процес обробки готівки. Представники банку вважають, що в процесі обробки готівки все ще існують труднощі, пов'язані з браком спілкування між різними відділами банку, оскільки обсяг готівки дуже великий. Виправити це вони планують, запровадивши в процеси технологію blockchain.

Нові можливості. Mastercard, наприклад, отримала патент на систему, яка зможе підтримувати різні види блокчейнів і здійснювати операції в декількох криптовалют. Mastercard планує тримати на одній блокчейн-платформі інформацію по різних типах транзакцій з віртуальними валютами. Для цього в компанії створили власну схему блоків, в якій різні блоки мережі можуть вміщати різний тип даних. Також блокчейн буде розділений таким чином, щоб отримувати дані по операціях з різних обчислювальних пристроїв.

Утворення. Дослідник з Оксфорда Джошуа Броггі оголосив про свої плани зі створення власного університету на Мальті, який буде побудований на технології blockchain. Таким чином, він планує істотно зменшити операційні витрати, шляхом автоматизації адміністративних процедур. Крім того, це дасть впевненість в реальності отриманої студентом освіти.

Стільниковий зв'язок. В рамках XBlockchain Summit, що проходить на Балі, був здійснений перший дзвінок за допомогою технології блокчейн. Це стало можливим завдяки пристрою XPhone, блокчейн-смартфону, який не потребує послуг мобільних операторів. Замість цього використовується власний блокчейн.

Таксі. У Китаї запустили безпечний сервіс таксі на блокчейні. Нова китайська платформа VV Go покликана вирішити складності із забезпеченням безпеки пасажирів таксі. Платформа на блокчейні зможе своєчасно і прозоро ділитися інформацією про водіїв і поїздках з усіма користувачами. Якщо пасажир, наприклад, зробить екстрений виклик, мережа дозволить іншим водіям і навіть поліції швидко зреагувати.

Керування автомобілем. Німецький виробник Infineon і компанія XAIN працюють над впровадженням технології блокчейн в автомобільну електроніку, щоб поліпшити системи кібербезпеки. Загалом, технологія блокчейн повинна надати власнику авто можливість управління правами доступу до тих або інших даних про машину. Крім того, власник авто зможе делегувати права доступу по блокчейн-мережі через мобільний додаток.

Незважаючи на всі свої плюси, blockchain-технологія також має ряд мінусів.

Таблиця 1.1 – Переваги та недоліки технології blockchain

Переваги	**Недоліки**
Денцентралізація - в усіх учасників рівні права	Масштабованість - повний розмір блокчейна буде рости з ростом числа операцій

Прозорість - дані знаходяться в публічному доступі, а їх видалення або зміна виключено.	Зловмисники - якщо транзакцію зроблено помилково, скасувати її буде неможливо
Універсальність - можливість застосування в абсолютно різних сферах життя	Можливе порушення цілісності, в разі, якщо 51% обчислювальних потужностей буде перебувати на одному пристрої
Надійність - необхідність перевірки операції всіма учасниками системи дає можливість «пропускати» тільки легітимні транзакції.	

З кожним днем використання blockchain стає все доступнішим. На сьогодні такі компанії як Amazon і Huawei надають можливість створення власних блокчейнів. Це дозволить людям, які хочуть створити власні блокчейн-мережі, заощадити значну кількість грошей, які їм би знадобилися для запуску мережі з нуля.

Крім того, університети не могли не відреагувати на необхідність в блокчейн-фахівцях на ринку праці. Тому американська Школа бізнесу Леонарда Н. Штерна вже оголосила про те, що створить курс підготовки професіоналів у цій сфері, які зможуть з легкістю вирішувати проблеми і завдання в сфері blockchain.

Розвиток і підтримка компаніями

VMware

Багато компанія зацікавлені у вивченні і розвитку технології блокчейн. Наприклад, в VMware був створений цілий дослідний відділ, який вивчає вплив блокчейна на область фінансових технологій в цілому. Ними було сформовано їх унікальне бачення, яке базується на п'яти пунктах:

- приватні розподілені системи зберігання без використання доказів роботи (PoW);
- високошвидкісна реплікація даних;
- світ безлічі блокчейнів, а не єдиної мережі;
- підтримка транзакцій з можливістю крос-операцій;
- вбудована можливість регулювання членства, не тільки authX / authZ.

Крім того, для користувачів послуг VMware є готове рішення BlockChain on vSphere, Яке дозволяє створити свою мережу в кілька простих кроків.

HyperLedger

У 2015 групою Linux Foundation був заснований зонтичний проект відкритого програмного забезпечення для блокчейна і супутніх інструментів – HyperLedger, який призначений для підтримки спільної розробки технологій розподіленого реєстру на базі блокчейн.

Проект HyperLedger також має власний дослідний центр, в якому акумулюється досвід багатьох компаній: від консалтингового та фінансового сектора до IT-гігантів.

NEO

NEO – це відкритий блокчейн для розумної економіки. Творці собі за мету ставлять розвиток екосистеми смарт контрактів на основі своєї мережі.

В основі NEO лежить модель доказів частки володіння (Proof-of-Stake), що дозволяє домогтися проведення до 10000 операцій в секунду. В якості застави використовується криптовалюта Neo, а для оплати комісій за проведення транзакцій використовується NeoGas, який створюється при отриманні нових блоків і розподіляється між власниками Neo.

В даний момент проходить конкурс розробників NEO з призовим фондом в 490000 $ в партнерстві з Microsoft. Учасникам пропонується представити прототип додатка використовує можливості розумних контрактів NEO.

Окремо варто відзначити наявність підтримки декількох мов програмування (C #, Python, Java), що дозволяє використовувати можливості блокчейна в уже існуючих системах і не витрачати час на вивчення нової мови.

На основі Neo можна реалізувати свій приватний блокчейн. Творець мережі відразу отримує в своє розпорядження 100 мільйонів Neo і може використовувати їх в якості валюти для додатків або інших цілей. Для обслуговування і початкового запуску мережі потрібно мінімум 4 машини, які можна створити в одній приватній хмарі.

У сфері фінансових інструментів Bitcoin, будучи першою масовою криптовалютою, безумовно показав як можна грати за новими правилами без посередників та управління зверху. Однак, можливо навіть більш важливим результатом появи Bitcoin стало створення технології блокчейн.

Блокчейн в силу своєї природи не є відповіддю на рішення всіх проблем, тому більша частина новоспечених компаній, які впроваджують цю технологію, швидше за все, зникне найближчим часом. Але саме блокчейн, як технологія, дозволяє організувати взаємодію віддалених учасників без контролюючого органу і там, де це буде затребувано, технологія знайде застосування.

В даний час найбільш актуальною темою в економіці і бізнесі є блокчейн. Блокчейн – це досить молода технологія з невеликою історією, яка у більшості людей асоціюється тільки з криптовалютою. Однак, сфера застосування блокчейн-технології обмежується не тільки фінансовим сектором. На основі даної технології створюються соціальні мережі, онлайн-системи для голосування, різні додатки для контролю ланцюжків поставок і т.п.

Незважаючи на перспективність, у даній технології є противники. Основною причиною цього є недостатнє розуміння блокчейн-технології. Тому в даний час постає необхідність розробки законодавчої бази і стандартів безпеки використання технології.

З 2016 року директор з досліджень міжнародного аналітичного агентства Gartner Деріл Пламмер перерахував на конференції Symposium / ITExpo десятку трендів розвитку міжнародної економіки та фінансів, які

об'єднані спільною темою – що відбувається цифровою революцією. Одним із трендів були позначені блокчейн-технології, як нове явище, здатне змінити глобальну економіку і фінанси.

Блокчейн (з англ. Blockchain – ланцюжок блоків) – це спосіб зберігання даних, а саме, безперервний послідовний ланцюжок блоків, що містять інформацію про транзакції, вибудуваний за певними правилами. У детальному плані це заснований на алгоритмах криптографічної системи загальнодоступний реєстр, в якому зберігаються дані про всі зміни і операції, що відбулися в системі.

Вперше блокчейн-технологія була реалізована в 2009 році в якості інструменту для проведення операцій з електронною валютою «bitcoin», тобто грала роль загального реєстру транзакцій.

В даний час технологія блокчейн розвивається як відокремлена технологія, яка може застосовуватися і за рамками систем криптовалюти.

Можна виділити 3 умовні області застосування блокчейн-технологій:

1. Фінансові транзакції на основі криптовалюти (наприклад, цифрові платежі на основі біткоїнів);

2. Контракти (застосування технології в області економіки, ринків і фінансів, а саме робота з акціями, облігаціями, заставами, ф'ючерсами, правовими титулами, активами і контрактами);

3. Область застосування в сфері державного управління, науки, освіти, охорони здоров'я та ін. (Застосування технології поза рамками фінансових транзакцій). [2]

При цьому використання даної технології має ряд переваг:

- Прозорість (за допомогою публічного або розподіленого зберігання), тобто доступ до всієї історії подій відкритий усім учасникам системи;
- Децентралізованість – зберігання даних на декількох серверах. На відміну від хмарних сховищ Google, Dropbox і ін., для доступу до даних знадобиться ключ шифрування, що забезпечить конфіденційність даних;
- Рівноправність. Технологія блокчейн не має на увазі адміністраторів (зберігачів інформації), а всі учасники мають однаковий статус і можливості;
- Безпека (застосування шифрування для підтвердження транзакцій).

Таким чином, блокчейн-технологія може істотно знизити можливість створення і використання шахрайських і корупційних схем, що дозволить забезпечити збереження громадських і державних інтересів.

У ряді країн технології блокчейн вже активно впроваджуються в сферах нерухомості, інтелектуальної власності, соціального забезпечення, охорони здоров'я і в пенсійній системі. Є блокчейн-рішення для проведення різних закупівельних процедур, голосування, ряду нотаріальних послуг.

Технологія блокчейн на Україні отримала назву технології розподіленого реєстру (Distributed ledger technology - DLT).

Спочатку все, що стосувалося цифрової валюти сприймалося державними структурами в багнети, були так само висловлювання за

введення кримінальної відповідальності за обіг криптовалюти. Але в даний час є передумови по використанню технології блокчейна на Україні.

Бізнес-спільнота також проявляє ініціативи зі створення робочих груп, консорціумів, координаційних центрів, покликаних стимулювати розвиток блокчейн-технологій.

Першою організацією на Україні зі сприяння розвитку блокчейн-технології стала некомерційна організація «Блокчейн-фонд». Вона з'явилася в жовтні 2016 року, і основною її метою є популяризація технології розподілених реєстрів у громадян, а також взаємодія з органами влади.

У червні 2016 року біржа стала першою українською фінансовою організацією стала учасником міжнародного блокчейн-консорціуму Hyper-Ledger. Експерти біржі активно вивчають перспективи застосування блокчейн-рішень в процесах проведення торгів, клірингу і розрахунків. Участь в консорціумі надає біржі доступ до міжнародної експертизи і передових розробок в області технології блокчейн, дає можливість брати участь у формулюванні і впровадженні міжнародних галузевих стандартів застосування блокчейн технологій.

У 2017 році була створена дочірня компанія Біржі "Інновації", яка займається розвитком інноваційних технологій і співпрацею з фінансовими установами. Також, в 2017 році відбулося перше розміщення випуску облігацій з використанням технології розподіленого реєстру.

У серпні 2017 року за ініціативою ТОВ «Національні інформаційні системи» (далі - ТОВ «НАІНС») агентство по метрології оголосило про формування нового комітету зі стандартизації «Програмно-апаратні засоби технологій розподіленого реєстру і блокчейн ».

Основною функцією даного комітету є стандартизація архітектури і онтології технології блокчейн, сфери його застосування, вимог до програмного забезпечення та програмно-апаратних засобів даної технології, а також до їх безпеки і конфіденційності.

Створення такого роду комітету сприятиме зростанню довіри до використання технології.

Сфери застосування технології блокчейн різні, але особливий інтерес розвиток технології розподіленого реєстру викликає, по-перше, у фінансовій галузі, оскільки дана технологія надає можливість використання блокчейн для перевірки, виконання та зберігання транзакцій.

Так, розробку блокчейна на базі Ethereum і створеної компанією BitFury блокчейн-платформи Exonum планує Зовнішекономбанк (ЗЕБ).

АКБ розробив систему віддаленої ідентифікації клієнтів на базі технології блокчейн від Microsoft. Нове рішення дозволить користуватися послугами інших банків без фізичного відвідування їх відділень. Про ініціації власних блокчейн-проектів заявили також Зовнішекономбанк і банк ВТБ.

За період з 2014-2017 Ощадбанк ініціював близько 15 різних пілотних проектів, пов'язаних з технологією блокчейн, деякі з яких не отримали подальшого розвитку і були припинені, а деякі перейшли в промислову

експлуатацію. Одним з таких проектів стала блокчейн-платформа Digital Ecosystem, яка дозволяє обмінюватися документами в зашифрованому вигляді за допомогою технології розподіленого реєстру. Платформа Digital Ecosystem вже була випробувана з рядом контрагентів, зокрема, з антимонопольною службою.

Ще один успішний проект реалізується «Ощадбанк Факторинг» спільно з «М. Відео ». Проект дозволив вирішити проблему звірки документів про постачання. Платформа на основі блокчейн в автоматичному режимі порівнює зашифровані дані по поставкам: якщо вони співпадають у обох учасників, поставка підтверджується. Такий підхід дозволив прискорити процес звірки, уникнути подвійних виплат по одній і тій же грошовій вимозі і виключити ризик витоку комерційно важливих даних.

Технологія блокчейн може зробити революцію в банківській сфері замінивши систему міжнародних розрахунків і платежів SWIFT. Технологія розподіленого реєстру може значно вдосконалити і здешевити транскордонні операції банків за рахунок усунення посередників, у яких є програмне забезпечення SWIFT.

Однак, на конференції Forbes, яка відбулася 28 лютого 2018 року, керуючий директор Sberbank CIB Сергій Поліканов, що заявив, що ринок поки не готовий до переходу від системи SWIFT, так як у платформи блокчейн існують проблеми з точки зору інформаційної безпеки.

Для України перехід від системи SWIFT до системи блокчейн так само має перевагу в зв'язку з тим, що з початку введення санкцій не раз піднімалася тема можливого відключення її від SWIFT. [12]

По-друге, блокчейн застосовується в сфері закупівель.

Завдяки даному сервісу учасники процесу зможуть фіксувати етапи виконання своїх зобов'язань за контрактом. Сервіс дозволить направляти сторонам повідомлення про настання планових подій, проводити перед закриттям контракту перевірку виконання сторонами зобов'язань, розраховувати штрафи.

Робота виконується через особистий кабінет сервісу, в якому учасники процесу фіксують етапи виконання зобов'язань. Сервіс направляє повідомлення сторонам про настання планових подій, проводить фінальну перевірку виконання сторонами всіх зобов'язань перед закриттям контракту, автоматично розраховує розмір можливих штрафів, а також надає контролюючим аналітичну звітність. Завдяки даній системі можна скоротити терміни узгодження і створити єдину базу документів виконання контрактів.

Також, Державний електронний майданчик «РТС-тендер» протестував систему єдиної акредитації учасників закупівель на всіх електронних майданчиках. Дана система була реалізована на базі вільного системного забезпечення MultiChain, і дозволяє здійснювати багаторазову верифікацію даних і виключення їх несанкціонованих змін. [11]

По-третє, блокчейн використовується в сфері реалізації прав на інтелектуальну власність.

Організація, яка забезпечує стійкість функціонування і розвиток децентралізованої мережі блоків транзакцій з правами і об'єктами інтелектуальної власності - розподіленого реєстру IPChain. З використанням IPChain будуються сервіси вільного обороту наукових творів, які дозволяють виплачувати справедливу винагороду авторам, сервіси продажу і придбання моделей для тривимірної друку з композитів і металів, банки даних генетичної інформації, сервіси отримання винагород за використання музичних творів у громадських місцях. [11]

По-четверте, блокчейн знайшов застосування в сфері охорони здоров'я.

У вересні 2017 року Міністерство охорони здоров'я заявило про плани перевести електронні карти пацієнтів в українських медичних установах в єдину систему довідок на базі блокчейна.

Громадяни зможуть самостійно вибирати, з ким вони поділяться особистими відомостями.[11]

По-п'яте, блокчейн використовується в сфері міської авіації.

Першим розробником літальних апаратів, який буде використовувати цю технологію, стане Bartini - компанія-резидент технопарку, який розробляє електрольоти вертикального зльоту і посадки, згідно з технічними характеристиками програми Uber Elevate. [14]

Впровадження блокчейн-платформи Blockchain.Aero в міський авіації і аеротаксі зробить можливими:

- Перехід до відкритих і автоматизованих бізнес-процесів, польоти на токенах, як поїздки на бензині в звичайному автомобілі (користувач здійснює транзакцію в токенах зі свого гаманця на гаманець машини, а та, в свою чергу, робить транзакцію на електрозаправках);
- Визначення вартості польоту з відкритого алгоритму, що враховує попит і пропозицію, а також витрата експлуатаційних матеріалів;
- Рішення проблем екології та міського трафіку, зокрема, за рахунок використання аеротаксі - альтернативи розвитку міського транспорту.

Незважаючи на наявність ряду успішних блокчейн-проектів, Український венчурний фонд відзначає нечисленність інвестування блокчейн-стартапів в Україні. Причину цього експерти фонду вбачають у відсутності розуміння своєї цільової аудиторії у вітчизняних компаній.

Одними з основних проблем, що гальмують впровадження блокчейн-технологій, можна виділити наступні:

- відсутність правової бази;
- відсутність правового регулювання застосовуваних в блокчейні підходів захисту інформації;
- відсутність єдиного арбітра, якому б всі довіряли (в державних системах цим арбітром виступає сама держава).

Виходячи з вищесказаного, можна зробити висновок, що в період з 2015-2017 року на Україні сформувалася розрізнена техносистема, що включає банківський сектор, комерційні компанії, неурядові організації та

асоціації, які здійснюють дослідження і розробки, пов'язані із застосуванням блокчейн-технологій.

На даний час в Україні немає єдиної правової бази регулювання технології блокчейн.

1.2 Система документообігу та документообміну на приватних підприємствах

Вітчизняні системи електронного документообігу (СЕД) вперше з'явилися ще в Радянському Союзі, в 80-х роках минулого століття. Робилися вони для державного сектора, а саме, для ЦК КПРС. Для початку була автоматизована робота загального відділу, а потім поступово, протягом декількох років, вся робота з документами ЦК і Політбюро. Ця система пізніше стала використовуватися в Апараті Президента СРСР і в Адміністрації Президента.

Офіційного визначення системи електронного документообігу (СЕД), затвердженого стандартом, не існує. По суті, СЕД – це система, що дозволяє автоматизувати основні процедури діловодства компанії. Вона охоплює процеси створення, обробки, тиражування, передачі, зберігання документів, контролю над їх виконанням і призначена для ефективного управління підприємством.

При впровадженні СЕД на підприємстві зазвичай ставлять такі цілі:

- скорочення або повна відмова від паперового документообігу;
- створення єдиної інформаційної бази компанії;
- зниження ризику втрати документа;
- структурування всієї документації по затвердженій номенклатурі;
- підвищення дисципліни серед співробітників завдяки можливості відстеження діяльності виконавця конкретного документа;
- контроль над виконанням документів відповідно до резолюцій керівника;
- підвищення ефективності роботи компанії.

СЕД – один з головних інформаційних ресурсів компанії, який використовується для роботи з різними видами і типами документів, що інтегрується з іншими діловими системами. Традиційний для СЕД функціонал, на думку експертів компанії «1С», розширюється в напрямку автоматизації спільної роботи співробітників.

Як і будь-який інструмент, СЕД потрібно застосовувати за призначенням і тоді, коли це дійсно необхідно компанії. Тільки в цьому випадку впровадження системи буде ефективно і принесе реальну користь.

Визначити ефективність впровадження СЕД в цифровому вираженні досить складно. Компанією DIRECTUM на основі власної методики були виділені ключові ефекти від впровадження СЕД на підприємстві [2]. При цьому величина ефекту залежить від того, чи є компанія великим

підприємством з декількома філіями або невеликим підприємством, розташованому в одному офісі. Потенційні вигоди наступні:

Зниження матеріальних витрат:

- невелике підприємство – на 5%;
- велике підприємство з декількома філіями – на 20%.

Така різниця обумовлена тим, що на підприємстві малого бізнесу робочі місця співробітників розташовані компактно, немає необхідності створювати велику кількість паперових копій документів.

Економія на базових процесах – вихідні і вхідні документи, організаційно-розпорядчий документообіг, контроль виконання доручень:

- невелика компанія – від 8 до 15%;
- велике підприємство – до 50%.

Окремо розглядається процес узгодження і виконання доручень. Тут економія може скласти від 6% до 23% в залежності від структури і величини компанії і стилю її роботи. Чим більше формалізовані процеси в компанії, тим вище буде ефект.

Економія на конкретних операціях, не прив'язаних до процесів, - пошук документів, забезпечення доступу до них і т.д. – від 3 до 24% в залежності від стилю роботи з документами і від організації системи їх зберігання. Якщо створити загальнодоступне сховище електронних документів з чітко прописаними регламентами роботи і зберігання, правами доступу до них, то ефект для компанії буде максимальним.

Зниження ризиків. Цей ефект стосується стратегічних показників і найменше піддається формальному розрахунку. У деяких випадках СЕД дозволяє знизити ризики прострочення узгодження та укладення договорів до 60%.

За оцінками експертів, впровадження СЕД на підприємстві окупається в середньому за термін від 3 місяців до 3 років [3].

На практиці установка систем електронного документообігу дозволяє домогтися реального зростання прибутку і ROI. Як приклад можна привести два кейса.

Кейс № 1 [4]

Клієнт – власник найбільшої компанії-виробника металочерепиці та профнастилу, має 76 підрозділів в різних містах країни. Для забезпечення структурованої і чіткої постановки завдань співробітникам і контролю над їх виконанням в організації була впроваджена система документообігу. У підсумку всіе бізнес-процеси компанії стали контрольованими, співробітники звільнилися від рутинних процесів документообігу, що підвищило продуктивність їх праці, на 30% скоротилося навантаження на секретаріат і кадровий відділ, швидкість документообігу збільшилася на 60%. Зростання продажів компанії склало 10%, додатковий прибуток – 100 млн грн, ROI - 1566%.

Кейс № 2 [5]

Установка СЕД в мережі гіпермаркетів товарів для будинку і дачі. Проблема полягала в тому, що вся переписка компанії з обговорення та узгодження договорів велася по електронній пошті, що нерідко призводило до втрати листів (наприклад, через банальну фільтрацію в спам) і зриву термінів. В результаті впровадження СЕД терміни узгодження договорів скоротилися на 30%, своєчасність проведення переговорів з постачальниками підвищилася на 35%, а результативність підписання комерційних умов зросла на 30%. Щодня в СЕД компанії створюється близько 50 документів, а в обробці знаходиться одночасно 700. Створена єдина інформаційна база, завдяки чому повністю виключені випадки втрати первинних документів. В системі працюють 900 користувачів, щодня ініціюється більше 40 заявок від підрозділів торгової мережі і 1800 знаходяться в стадії активної обробки. Виручка компанії виросла на 250 млн грн., додатковий прибуток склав 42,5 млн грн, ROI проекту впровадження – 254%.

Види систем електронного документообігу

Хоча будь-яка класифікація є умовною, традиційно виділяють кілька видів СЕД по функціоналу і важливістю справ:

Системи діловодства. Вони використовуються в організаціях з жорстко формалізованими правилами документообігу і вертикальним керуванням незалежно від їх розміру, форми власності та виду діяльності. З їх допомогою можна вирішити кілька основних завдань:

- упорядкувати роботу з кореспонденцією, як виходить, так і входить;
- оптимально організувати рух внутрішніх документів в компанії;
- налагодити роботу зі зверненнями клієнтів;
- організувати внутрішній електронний архів документів.

По суті, вони є спадкоємцями паперового діловодства.

Електронні архіви. Це системи структурованого зберігання документів, що забезпечують надійність зберігання, розмежування прав доступу, зручний і швидкий пошук. Впровадження систем такого типу зазвичай це пов'язано з потребою структурування електронної інформації, незалежно від виду документів – текстовий, графіка, мультимедіа. Основні функції архіву – оцифровка паперових документів, управління web -контентом, потоковий ввід і швидкий пошук. Завдяки впровадженню архіву можна скоротити час доступу до інформації, знизити ризики псування або втрати важливих документів, підвищити рівні інформаційної безпеки. Електронні архіви зазвичай існують в складі СЕД і окремо використовуються досить рідко.

Workflow-системи забезпечують автоматизацію не окремих функцій, а бізнес-процесів компанії. Дослівний переклад Workflow – «потік робіт». Система Workflow чітко визначає процес: що, хто, коли і як робить, звідки отримує і куди відправляє. Користувачеві не потрібно замислюватися над тим, як створити документ, як його отримати, як обробити, в які терміни і кому відправити – все вже закріплено в системі. Співробітник не зможе неправильно заповнити документ, пропустити якісь терміни, в системі

передбачені нагадування, а також повідомлення керівника про те, що на конкретному етапі у конкретного користувача процес обробки документа порушений. Є можливість оцінити причини допущення помилок і своєчасно їх усунути. Workflow-системи в основному встановлюють в компаніях з високим ступенем формалізації бізнес-процесів, документообіг в яких при простій структурі має масовий характер. Мінусом таких систем є складність і тривалість застосування. Крім того, вони не можуть замінити електронний архів, оскільки зберігають не всі документи, а тільки використовувані в процесі роботи.

ЄСМ-системи використовуються для збору, управління, зберігання інформації (контенту) і надання до неї доступу співробітникам компанії, тобто, на перший погляд, виконують ті ж самі функції, що і попередні системи. Однак істотна відмінність ЄСМ – систем від своїх побратимів в тому, що вони дозволяють працювати як зі структурованим, так і з неструктурованих контентом і мають більш гнучкий функціонал. По суті, забезпечення електронного документообігу є тільки однією з функцій ЄСМ разом з управлінням файлами і записами, управлінням знаннями, власне Workflow, і управлінням web -контентом. У деяких ЄСМ-систем також є функція CRM і управління завданнями і дорученнями.

1.3 Сучасний стан ринку для криптовалют

У 2010-х роках весь фінансовий світ був зацікавлений новим видом грошей – криптовалюта.

З'явилися криптогроші в зв'язку з масштабним розвитком інтернет-магазинів, транзакції яких вимагали певного рівня довіри. Гарантувати таку довіру міг посередник – у багатьох випадках фінансовий інститут. Зворотною стороною таких гарантій стала можливість скасування операції перерахування грошей, що створювало перешкоди для гарантій продавця, що він отримає свої гроші.

Рішенням стала інтернет-технологія, яка змінила підходи до формування грошових систем та організації грошового обороту в мережі і породила нову валюту – інтернет-монети. Тепер і в Інтернеті з'явилася власна валюта – біткоїни. Якщо взяти в порівняння біткоїни і звичайні валюти, то можна зробити безсумнівну висновок, що в залежності від місця перебування в будь-якій країні, доводиться розплачуватися тією чи іншою валютою, а біткоїнами користувачів Інтернету ніхто розплачуватися не примушує і користування криптовалютою абсолютно добровільне.

Одиниця віртуальної валюти, яка представляє собою закодовану інформацію, застрахована від підробки і не піддається копіюванню є монета (англ.-coin). Відмінність електронної криптовалюти від звичайних грошей в електронному вигляді полягає в тому, що в реальному житті для поповнення електронного балансу необхідно спочатку внести звичайні гроші в фізичному вигляді на рахунок через банк або банкомат. Отже, для звичайної валюти

електронний вигляд – це одна з форм уявлення. Криптовалюта ніяк не пов'язана ні з державною валютною системою, ні з будь-якою іншою звичайною валютою, вона емітується тільки в мережі.

Будь-яка людина, яка має комп'ютерне обладнання потрібної потужності і володіє певним програмним забезпеченням може зайнятися Майнінгом. Видобуток монети, набору зашифрованої інформації, відбувається в процесі, коли обчислювальні потужності комп'ютера вирішують певні алгоритми, з умовою постійного збільшення складності алгоритму. Доказом того, що в мережі монета є в наявності, служить обліковий запис – технологія блокчейн. Зберігається ця валюта розподіленою по електронним кріптовалютним гаманцях, децентралізовано.

«Bitcoin» є первинною сходинкою створення історії криптовалюти. Біткоїн починався з концепції – документа, який потрапив до друку 31 жовтня 2008 року, підписаного невідомою особою, яка працювала під псевдонімом Сатоши Накамото (Satoshi Nakamoto). Хто є справжнім творцем, група людей чи все ж одна людина – до сих пір залишається невідомим, незважаючи на багаторазові журналістські розслідування. Днем народженням біткоїнів вважається день, коли був створений найперший блок в мережі (генезис-блок), а точніше 03.10.2009 в 18:45 за Гринвічем. Цей день відзначається безсумнівно співтовариством по всьому світу.

Існує кілька особливостей Bitcoin, які дозволяють відрізнити його від інших видів електронних і паперових грошей.

Першою особливістю є доступність і децентралізація. Мережа Bitcoin це комбінація всіх клієнтських програм і бази даних з розподіленими параметрами «blockchain», яка є на будь-якому комп'ютері, де встановлений пакет спеціалізованого обладнання, що володіє повним функціоналом. Технологія блокчейн являє собою повністю відкритий для громадськості і перегляду записаний реєстр всіх операцій в системі. За допомогою софт-оболонки спеціальних сервісів відстеження або власного гаманця, можна підключиться до реєстру, в незалежності від місця перебування, з будь-якої точки світу, без авторизації і паролів.

Далі слідує повна прозорість розрахунків. Маючи тільки адреса Bitcoin можна не тільки дізнатися про всі транзакції, а ще й вивчити історію кожного платежу (теоретично), до моменту генерації монет, при тому, що він ніколи не буде ліквідовано з бази даних.

Також можна виділити вільний вибір ступеня участі. Є можливість встановити офіційний клієнт Bitcoin Core, який зберігає всю історію транзакцій. Або ж встановити один з простих або мобільних гаманців, якщо не потрібен аналіз blockchain і автономна робота.

Наступною особливістю є ні що інше, як відсутність контролю за самою мережею, в якій відбуваються транзакції. Так як система блокчейн – є розподіленою базою даних, створеною на основі рівноправних вузлів, мережа біткоіни не має центрального контролюючого органу, який може фактично заморозити будь-який рахунок, видалити або змінити-скасувати

транзакцію, змінити кількість грошових одиниць в системі, заблокувати або скасувати платіж. Існують невеликі комісійні винагороди, що не залежать від суми транзакції і практично не відчутні при здійсненні операції. Всі угоди в блокчейн-системі є безповоротними так само, як і операції з готівкою / грошима.

Неповторність Bitcoin полягає також в можливість анонімних розрахунків. Біткоїн це легкий і анонімний засіб розрахунків. В якому, для відкриття номера рахунку в системі, не потрібно ніяких документів. Це рядок довжиною близько 34 символів з цифр і букв латинського алфавіту в різному регістрі.

Нарешті, найголовнішою відмінною рисою Bitcoin є неперевершений захист. На сьогоднішній день Bitcoin – це мережа децентралізованих обчислювальних потужностей, загальна продуктивність якої більш ніж в 8 разів (по швидкості розрахунку хеш SHA-256) перевищує сумарну обчислювальну потужність всіх суперкомп'ютерів у світі. Технологія блокчейн влаштована таким чином, що виключає централізований контроль і зміну даних, щоб захопити над нею навіть обмежений контроль, потрібні величезні комп'ютерні потужності і ресурси і витрати в сотні мільйонів доларів. Але, не дивлячись на все вище сказане, не можна не виділити деякі недоробки, які необхідно вирішити для повного впровадження Bitcoin в економічну систему країни.

По-перше, це довіра до Bitcoin. Екосистема цієї криптовалюти залежить від ключових гравців, без яких неможлива нормальна робота в мережі. Це провайдери гаманців, майнингові пули, криптовалютні біржі, платіжні оператори. Вони можуть спільно прийняти вигідне тільки для них рішення, заради прибутку, але не зважаючи на те, що від цього постраждають звичайні користувачі. В таких випадках ні уряд, ні суд, не зможуть змусити їх дотримуватися будь-які правил [1].

Певні держави дали цій криптовалюті офіційний статус і видали нормативні документи, що коректують роботу кріптовалютних бірж, але біткоїн-компанії, як правило, сприймають контроль над собою негативно і залишають ринок.

Все це означає, що біткоїни вимагає не меншої довіри, ніж національні валюти. Тому, стверджувати про те, що власники електронних валют можуть бути спокійні за свої заощадження, недоречно.

По-друге, це проблема малодоступності. Не можна забувати, що біткоїни є віртуальною та тому повністю залежною від комп'ютерів. Там, де немає зв'язку з Інтернетом, не може і бути Біткоїнів.

По-третє, є такою, що важко добувається. Суть видобутку монет Bitcoin є вирішенням складного криптографічного завдання, для якого невідомо кращого підходу ніж брутфорс. Видобуваються монети не по одному біткоїну, а по блокам або ж «пачкам». Спочатку розмір заробляє блок, що становить 50 BTC, але потім він знизився вдвічі після кожних 210 тис. добутих блоків. В даний момент система вже включає більше 250 тис.

добутих блоків, отже, один блок приносить близько 25 BTC. Через періодичне зменшення нагороди за блок, загальна кількість BTC ніколи не перевищить 21млн, ~ 55% всіх BTC вже видобутих і, за прогнозами, ця цифра досягне 99% до 2032 року [2].

Періодично, через кожні 2016 здобутих блоків, відбувається коригування складності їх видобутку.

Поки вартість видобутих BTC перевищує витрати на обладнання і електроенергію, видобуток біткоїнів має сенс.

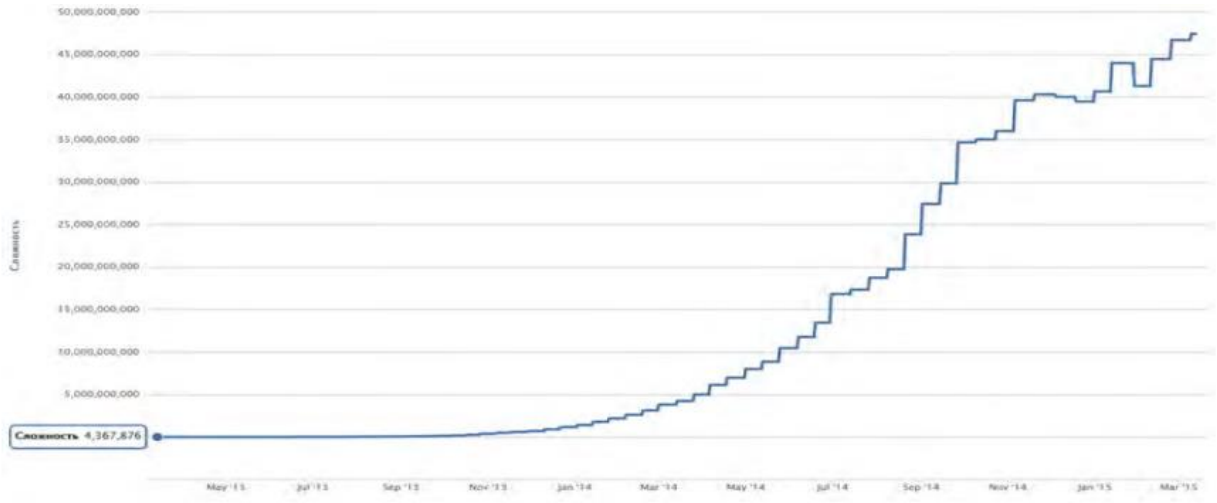


Рисунок 1.3 – Графік складності видобутку Bitcoin

По-четверте, до того ж, однією з головних проблем, є невідомість широким масам. Так як більшість людей до сих пір не знають про Bitcoin, як про реально існуючу валюту.

Таблиця 1.2 – Список найбільш затребуваних крипто валют

Крипто-валюта	Символ	Ціна, BTC	Об’єм 24, BTC	Всього монет	Рік
Bitcoin	BTC	1	11314.5519	21000000	2009
Ethereum	ETH	0,0158	83.7683	~90000000	2015
itecoin	L LTC	0,0057	5.8992	84000000	2011
MonaCoin	MONA	0,0000411	3.1766	105120000	2013
Ripple	XRP	-	3.0998	100000000000	2013

На сьогоднішній день, відомо про існування більше 92 різних криптовалют. Природно, в зв'язку з обставинами не всі вони користуються широким попитам, однак вони можуть нас здивувати на протязі 2-3років [3].

Світовій спільноті знадобилося всього лише пару років, щоб зрозуміти і дати оцінку такому поняттю, як криптовалюта. На думку деяких вчених, з віртуальних грошей швидко утворився приголомшливо величезний за своїми розмірами ринок, а також нова ідеологія грошей і повноцінна криптоекономіка [3]. Bitcoin, як першооснова, Litecoin і достаток інших криптовалют нині привертають вигідними перспективами, а також високою

рентабельністю, які привели до утворення 15-тимільярдного валютного ринку, побудованого за новими законами і засадам.

Обмінювати криптовалюту на реальні гроші слід на біржах, що надають цей вид послуг.

Деякі майданчики дозволяють замовити виведення коштів з особистого кабінету на електронні гаманці Webmoney, Kiwi, Яндекс.Деньги.

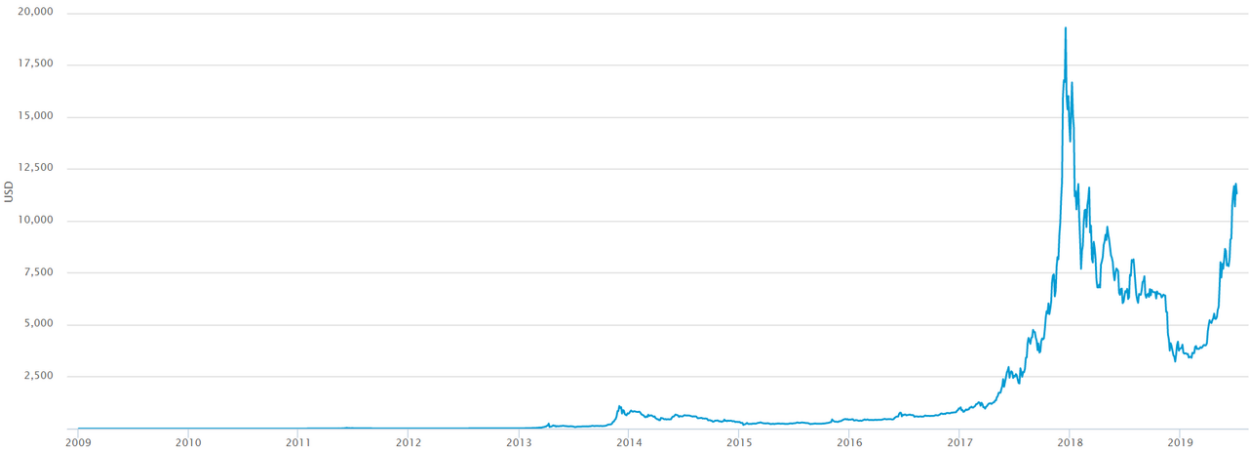


Рисунок 1.4 – Лінійний графік зміни курсу Bitcoin по відношенню до USD

Не можна не помітити, що якщо врахувати всі можливі ризики і намагатися не зберігати занадто великі суми грошей на електронних рахунках, то торгівля на біржах може стати вигідною справою для власника криптовалюти. Але, також слід враховувати, що при створенні віртуальних грошей за допомогою програм «Майнінг», витрачені ресурси на роботу комп'ютера не повинні перевищувати розмір потенційного прибутку від виведення монет.

Рисунок 1.5 – Логарифмічний графік курсу Bitcoin по відношенню до USD і показник волатильності

В даний час вже деякі країни схвалили криптовалюту. Є як явне схвалення з боку декількох штатів США, а також і з боку Нової Зеландії, Німеччини, Сінгапуру, Нідерландів, Австралії, а так і серйозні обмеження,

які можуть з часом перейти в заборонені заходи, це країни такі, як Україна, Росія, Китай та Індонезія.

Багато ж держав вирішили з обережністю поспостерігати за лінією розвитку біткоїнів, але все-таки дивлячись на нього з оптимістичної точки зору-це Канада і Швейцарія, країни Південно-Східної Азії і більшість країн Євросоюзу, Великобританія і Японія, а також федеральний уряд США.

Таким чином, це все, в зайвий раз, доводить те, що за віртуальними валютами, зокрема за біткоїн, благополучне майбутнє. Не дивлячись, на все ще, малодоступність і невідомість, інтенсивно розвивається ринок криптовалюти, що призведе до поліпшення життя не тільки в країні, але і у всьому світі, а також до вдосконалення економіки.

1.4 Постановка завдання дослідження

Останнім часом в світі і в економіці стали набирати популярність технології блокчейн (Blockchain), які стають все більш популярними, охоплюючи все нові сфери. Можна сміливо сказати, що перед ними лежить велике майбутнє. Перше, що спадає на думку при згадці технології блокчейн – це криптовалюта (біткоіни, Ванкоін та інше). Криптовалюта – це різновид цифрової валюти, створення і контроль за якою базуються на криптографічних методах і схемою доказів виконання якоїсь діяльності. Криптовалюта дуже популярна, однак не є головним і основним напрямком розробки в блокчейн, незважаючи на те, що знаходиться на слуху. Дуже скоро всі потенційні користувачі оцінять переваги даної технології і почнуть вводити в її роботу.

У загальному і цілому, технологія блокчейн являє собою розподілену систему записів, які пов'язані між собою, підтверджені і можуть легко бути перевірені. Описувати ці записи можуть все, що завгодно – від грошових переказів до укладених контрактів. Головне, що інформація в цих записах повинна бути підтвердженою, перевіреною і просто надійною.

Суть технології полягає в тому, що блокчейн – це величезна розподілена база даних загального користування [1]. У ній немає центрального керівництва, перевіркою транзакцій займається особлива категорія користувачів, звана Майнер. Майнери підтверджують справжність скоєних транзакцій і формують з них блоки, які шикуються в ланцюжки. Побудова заснована на тому, що кожен наступний блок містить інформацію про попередній. У відсутності посередників криється основна перевага технології. На даний момент всі операції з грошима, документами та іншими даними вимагають наявності посередників, які перевіряють справжність проведених операцій.

У блокчейні ж транзакції перевіряються і підтверджуються учасниками системи. Програмний код мережі доступний всім, і будь-хто може подивитися дані по операціях транзакцій – всі, крім конфіденційних: особистості власника і його персональних даних.

Завдяки своїй розподіленості, пов'язаності, підтвердження і можливості перевірки блокчейн забезпечує наступні якості:

Доступність. Системою можна скористатися всюди і завжди, де є інтернет, оскільки відсутність постійних адміністраторів тягне за собою відсутність перерв, а розподіленість має на увазі відсутність технологічних збоїв.

Незалежність. Завдяки пристрою мережі користувачі не потребують жодних посередників у вигляді нотаріусів, юристів, банків або платіжних систем.

Захищеність. Одного разу зроблений запис неможливо підробити або видалити.

На даний момент для здійснення будь-яких платежів і переказів потрібен банк або платіжна система. Вони в багатьох випадках вимагають комісію за проведення операцій і встановлюють свої правила і процедури звернення. Крім того, завжди є можливість розкрадання коштів з рахунку шахраями або навіть самим посередником. Також клієнти можуть зіткнутися з різними збоями в роботі інформаційних систем посередника або з тим, що посередник втратить ліцензію на свою діяльність.

Блокчейн дозволяє уникнути таких випадків. Всі платежі і переклади фіксуються у кількох учасників ланцюга, завдяки чому вкрасти або витратити гроші з рахунку його власника не вийде без цифрового підпису самого власника. Саме завдяки цим особливостям технології блокчейн стало можливим створення біткойнів.

Ще одна особливість цієї технології – можливість проводити умовні платежі.

Наприклад, можна зробити платіж з умовою, що він пройде, якщо його акцептує користувач із заданим ключем. Це, зокрема, виключає можливість обману при роботі з повністю цифровими продуктами, такими як ліцензії, відео, музика, будь-які види доступу: покупець не отримає продукт, якщо не сплатить, а продавець не отримає грошей, якщо не віддасть продукт.

Інші варіанти застосування умов - платіж «першого, хто виконає умову» або «тому, хто володіє потрібним ресурсом ». Ще одна незвичайна можливість - це мікроплатежі, такі, як посекундна плата за перегляд відео або прослуховування музики, оплата кожного рекламного показу, кліка, лайка або навіть смайлика.

По суті бонуси працюють так само, як і гроші, тому всі переваги блокчейна стосовно до них справедливі і для бонусів. Споживач може бути спокійний: його накопичення нікуди не зникнуть і не витратяться без його відома. Крім цього, доступність записів дає всім учасникам можливість бачити історію використання бонусів усіма учасниками системи, і користувачі зможуть бути впевнені в справедливості її роботи. Що стосується компаній-роздавальників бонусів, то вони теж отримують переваги від використання блокчейна. Наприклад, управління передачею

бонусів третім особам, або обмеження в їх використанні на умови придбанняпевних товарів і послуг.

Як вже говорилося вище, блокчейн має високу надійність і захищеність. Тому технологія прекрасно підходить для перевірки автентичності користувача. Перевірка підтверджує, що користувач володіє актуальним і коректним ключем для доступу до системи. На жаль, захистити володаря ключа від його крадіжки така технологія зможе не більше, ніж будь-яка інша; як відомо, найлегше отримати ключ від користувача не за допомогою злому, а методами соціальної інженерії. А ось від проникнення в систему і розкрадання даних шляхом злому або обману систем доступу блокчейн може захистити.

Розподіленість системи обумовлює практичну неможливість її злому. Спроба підробки записів теж буде швидко розкрита завдяки тому, що тільки підтверджені, правильні блоки записів поширюються між користувачами. За допомогою технології блокчейн можна створити систему аутентифікації для клієнтів банків, яка дозволить їм захищено входити в мобільний та інтернет-банк або здійснювати особливо критичні операції у відділеннях. Таким же шляхом можна аутентифікувати і співробітників банку при доступі до корпоративних систем. З цієї ж технології можна надавати банкам-партнерам і технологічним компаніям надійний доступ до банківських систем і даним.

Інший напрямок, що вимагає аутентифікації користувачів і набирає популярність - Інтернет речей. Поступово він все сильніше проникає в повсякденне життя, і з'являється неординарне завдання підтвердження автентичності за участю неживих користувачів мережі.

Наприклад, власнику автомобіля повинна бути надана можливість підключитися до нього, так само як і співробітникові техпідтримки; у зловмисника, навпаки, такої можливості бути не повинно.

Крім того, власник автомобіля повинен підключатися саме до свого майна, а не до чужого.

Вже на сьогодні широко поширені різноманітні контролери домашньої автоматизації, керуючі кліматом і інженерною інфраструктурою будинку. У багатьох автомобілях встановлені системи для контролю поведінки водія. Різні датчики і автоматичні системи стали невід'ємною частиною виробництва.

Однак аутентифікація потрібна не тільки людям або машинам. Один з найбільш природних додатків – перевірка достовірності документів. Ліцензії, права і сертифікати, дипломи, контракти і посвідчення особи, довідки, звіти та виписки, а ще твори мистецтва, винаходи і відкриття – все це можна фіксувати в blockchain.

Нерідкі випадки, коли шахраї підробляють неіснуючі в реальності заставні активи, продають кредитні автомобілі та іпотечні квартири. Особливості технології блокчейн дозволяють не допускати таких можливостей зловмисникам. Користувачам технології доступний самий актуальний і достовірний статус активу, відомості про те, кому він належить,

разом з докладною історією зміни власників, а також в яких діючі контракти бере участь зараз і в яких вже виконаних контрактах брав участь раніше.

Звичайно, у користувачів є можливість зберігати анонімність і приховувати свої персональні дані. При цьому вони завжди можуть перевірити, чи дійсно вони мають справу з реальним власником активу і чи володіє він усіма належними правами.

Здійснити таке застосування блокчейна досить легко, оскільки багато активів володіють унікальним ідентифікатором (номер свідоцтва про реєстрацію, кадастровий номер, серійний номер або навіть набір номерів ключових вузлів і агрегатів). Завдяки цьому навіть неповний реєстр, використовуваний лише кількома учасниками, буде корисний і вигідний. А потім його можна розширити і легко підключати нових користувачів [2].

Природно, вищеописаними прикладами область застосування blockchain зовсім обмежується. Замість побудови складних MDM-систем компанії можуть використовувати технологію blockchain для управління клієнтськими даними. Так само можна зберігати фінансову інформацію, щоб бути впевненим у достовірності бухгалтерських і податкових звітів, а також знати, хто і коли ці дані змінював виправними проводками і подачею коригувальних декларацій.

За допомогою блокчейна можна забезпечити контроль витрачання бюджетних або кредитних коштів. Користувачі можуть бути впевнені, що кошти не будуть неправомірно витрачені не тільки самим одержувачем, а й будь-яким його контрагентом. Наприклад, зараз нерідкі випадки, коли компанія бере кредит під закупівлю сировини, перераховує гроші постачальнику, який замість поставки товару виводить їх за кордон. Технологія блокчейна надійно захищає своїх користувачів від таких вчинків.

Ще блокчейн добре підходить для фіксування угод купівлі-продажу акцій та інших фінансових інструментів, а також в якості сховища даних про пенсійні накопичення і їх використанні фондами і керуючими компаніями [2].

Можливості технології блокчейн досить багатогранні, і можна придумати ще безліч цікавих, корисних і вигідних застосувань цієї технології. Перспективність її полягає ще і в тому, що будь-які ініціативи можуть бути розпочаті невеликою групою або навіть одним учасником для своїх клієнтів, а потім без особливих зусиль поширені на весь ринок.

У рамках даної дипломної роботи, враховуючи все вищевикладене, необхідно розробити захищене сховище інформації на базі технології блокчеїн.

Рішення повинно забезпечувати зберігання інформації без можливості модифікації (крім повного стирання всіх даних). Рішення повинно дозволяти зберігати довільний набір даних у вигляді рядка розміром до 5 МБ. Крім того, необхідно реалізувати рольову модель користувачів і можливість поділу даних, що зберігаються за типом.

Висновки до розділу

Технологія блокчеїн є універсальним способом зберігання і обробки інформації майже в будь-якій сфері діяльності, що сприяє формуванню нових крипто-інститутів і крипто-індустрій. Вже очевидно, що ця технологія і ті зміни, які вона в собі несе, революційна і призведе до глобальних світових змін. Блокчеїн надасть широкий вплив на фінансові ринки і такі сфери, як платежі, банкінг, розрахунки з цінних паперів, кібербезпека, брокерська звітність, аналіз торгів і прогнозування.

Ця технологія може дати державним органам нові інструменти, які дозволять скоротити обсяги шахрайства, число помилок і зменшити витрати на паперовий документообіг; великий потенціал для створення нових способів забезпечення прав власності і підтвердження походження товарів та інтелектуальної власності.

Технологія впливає на розробку і створення сервісів для продажу певних послуг, створюються спеціалізовані блокчеїн-консорціуми, які допомагають у вивченні технології та впровадженні її в крипто-індустрію.

На основі впровадження блокчеїн-технології очікується поява нових бізнес-сценаріїв, здатних трансформувати цілі галузі – починаючи з фінансів і закінчуючи охороною здоров'я. Блокчеїн може істотно підвищити податкову дисципліну. Блокчеїн торкається питань розвитку технології, операційної діяльності та трудових ресурсів. Він піднімає нові податкові, юридичні та нормативно-правові питання. Технологія блокчеїн становить загрозу для бізнесу спеціалізованого ПЗ.

Вона може прискорити розвиток розподілених хмарних систем, економіки спільного використання та Інтернет.

Застосування блокчеїн знизить витрати компанії на підготовку звітності, підвищивши її прозорість. Багато галузей вже мають пілотні проекти, які здатні скоротити витрати бізнес-процесів і підвищити ефективність транзакцій. Блокчеїн технологія генерує абсолютно нові бізнес-сценарії, які в майбутньому не тільки повністю перетворять цілі галузі, а й призведуть до зникнення деяких, наприклад, таких як посередництво. Радикальні зміни охоплять бізнес-моделі і процеси, ланцюжки поставок і відносини компаній з клієнтами у всіх секторах економіки.

РОЗДІЛ 2
МЕТОДИЧНІ АСПЕКТИ ПРОЕКТУВАННЯ СИСТЕМИ ДОКУМЕНТООБІГУ ТА ДОКУМЕНТООБМІНУ НА ПРИВАТНОМУ ПІДПРИЄМСТІ ЗА ДОПОМОГОЮ КРИПТОГРАФІЇ ТА ТЕХНОЛОГІЇЇ BLOCKCHAIN

2.1 Алгоритм реалізації системи документообігу та документообміну за допомогою криптографії та технології blockchain

Алгоритм реалізації системи документообігу та документообміну за допомогою криптографії та технології blockchain будується на формуванні блоків з даних, що вводяться. В даному блоці міститься додаткова службова інформація, яка необхідна для забезпечення цілісності і незмінності введених даних, а також для роботи самого ланцюжка блоків. Сам по собі ланцюжок блоків дуже схожий за структурою на однозв'язний список (рис. 2.1).

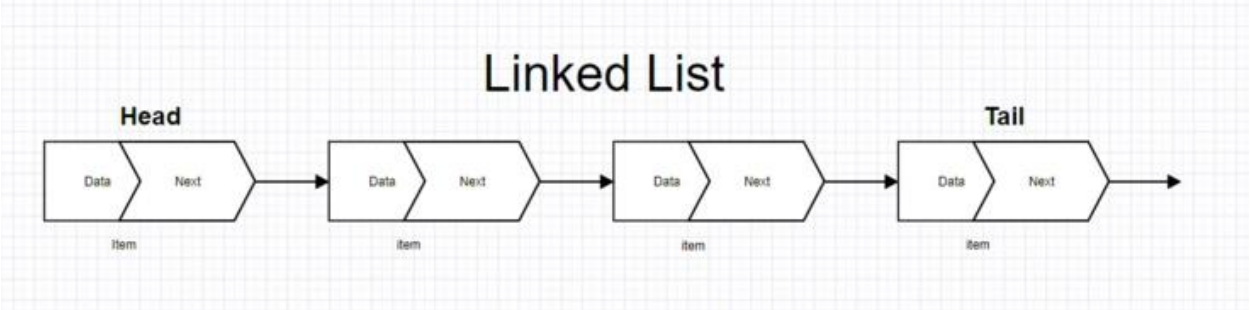


Рисунок 2.1 – Ланцюг блоків

Структура блоків blockchain наведена на рис. 2.2.

Блок даних містить наступні важливі поля:

Data – поле, в якому збережені самі корисні дані. Це може бути як простий рядок, так і більш складні структури.

CreatedOn – дата і час створення блоку даних. Важливо використовувати універсальний UTC час, щоб не виникало конфліктів через різні часові пояси.

Hash – унікальний ключ, створений на основі даних, що зберігаються у блоці за допомогою спеціалізованої хеш-функції, яка має на увазі тільки одностороннє шифрування.

PreviousHash – покажчик на попередньому хеш-блоці. Це необхідно для зв'язування блоків в єдиний ланцюжок.

Також можливе використання і додаткових даних, в даному випадку також використовуються наступні поля:

User – дані про користувача, який створив блок

Algorithm – використовуваний алгоритм хешування

Version – версія блоку

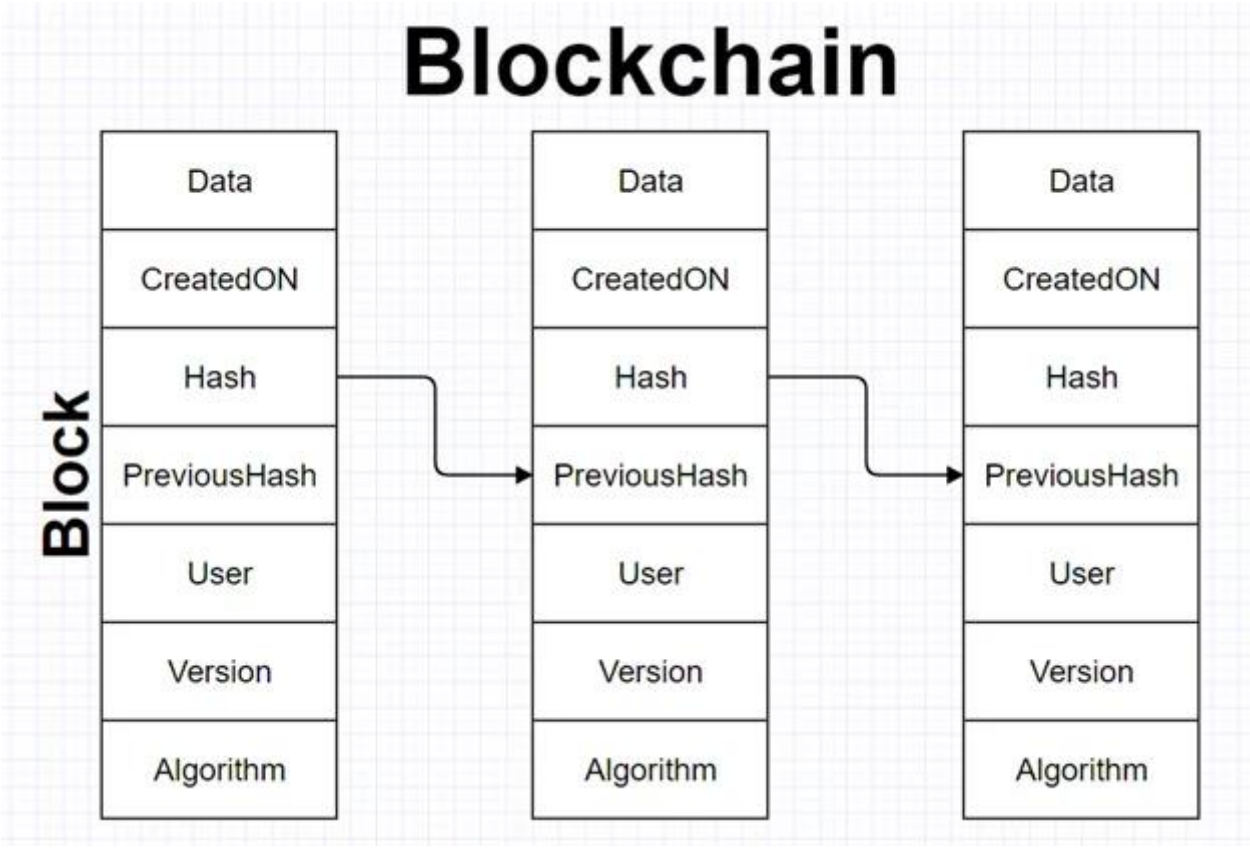


Рисунок 2.2 – Структура блоків blockchain

При створенні блоку даних виконується хешування введених даних. Потім виконується хешування всіх збережених даних блоку, після чого цей результат записується в поле Hash. Даний підхід дозволяє гарантувати збереження даних, тому що при зміні будь-якого з полів блоку хоча б на один символ хеш функція поверне зовсім інший результат, і система легко зможе це визначити, виконавши повторне хешування блоку і порівнявши зі збереженим хешем. При цьому кожен блок залежить від хешу попереднього блоку, в результаті чого при зміні будь-якого блоку в ланцюжку, весь ланцюжок стає некоректним.

Хешування – це процес перетворення вхідних даних довільної довжини в значення певного формату, шляхом перетворення за заданим алгоритмом. Основна особливість хеш-функції це можливість легкого перетворення вхідних даних в хеш, і неможливість однозначного відновлення вихідних даних з хешу.

Розглянемо приклад найелементарнішої хеш-функції, це підсумовування всіх цифр числа. Наприклад, якщо на вхід ми отримаємо число 73, то хешем даного числа буде 7 + 3 = 10. Це дуже проста операція, яка дозволяє отримати хеш. Але ось зворотне перетворення однозначно виконати неможливо, так як існує велика кількість чисел, що дають такий же результат: 64, 37, 181, 11116 і так далі.

Звичайно ж, це дуже простий приклад, і справжні хеш функції набагато складніше, але принцип роботи у них всіх ідентичний – отримання ключа на

основі вхідних даних, за умови, що навіть мінімальна зміна вхідних даних призведе до зміни ключа.

2.2 Математичний аспект дослідження

Основним напрямком розвитку блокчейн є застосування нових алгоритмів розподіленого доступу при генерації чергового блоку в ланцюжку блоків транзакцій. Недоліками існуючих алгоритмів «proof-ofworks» є їх обмеження по швидкості і складності здійснення транзакцій, пов'язаних з формуванням «обчислювальних пулів» Майнінг, високою ціною Майнінг і принципової неточністю опису складності обчислювальної здатності учасників блокчейна. Крім цього постійне зростання обчислювальної складності «Майнінг» починає обмежувати децентралізацію. Саме це викликає переходи до інших алгоритмам угоди при формуванні та верифікації нових блоків в блокчейне, таких як «proofof-stake» або «proofof-activity»[5]. Але простий перехід до консенсусу «наявності долейставок» веде до зниження стійкості протоколу консенсусу [3], а тривіальне об'єднання підходів «proof-of-works» і «proof-of-stake» на базі самих «stake-ставок» слабо здійснено на практиці [6].

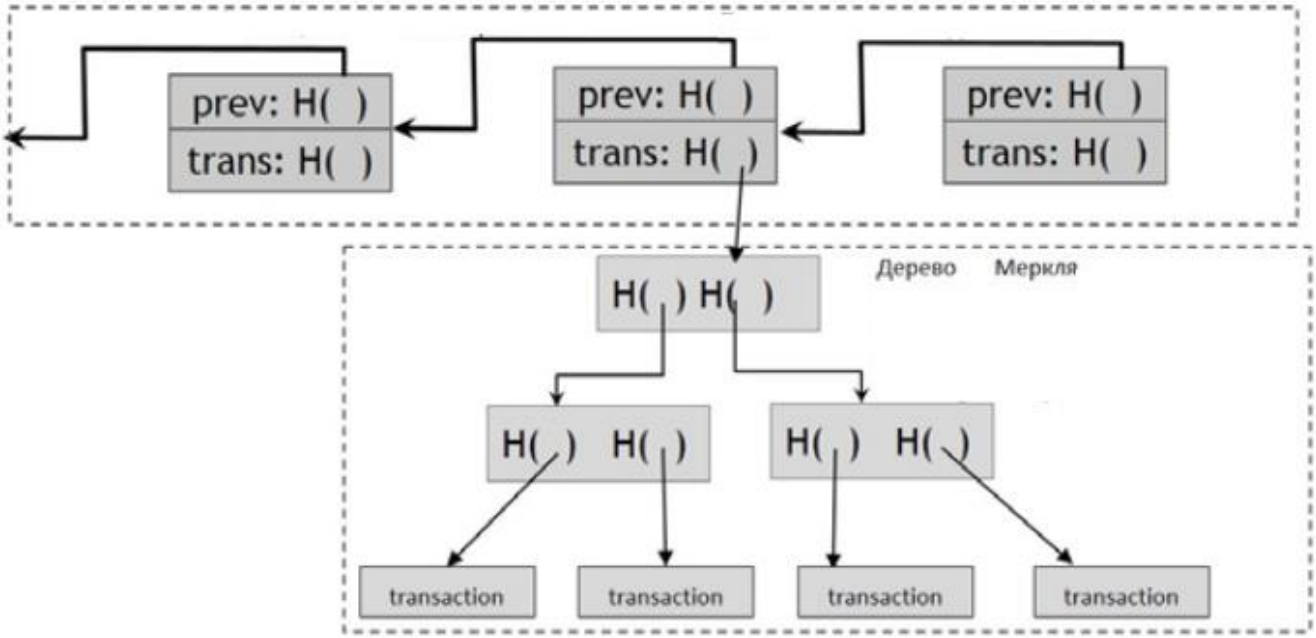
Ідея запропонованого алгоритму в тому, щоб для обчислення складної функції були потрібні не тільки обчислювальні ресурси, а й інформація про вхідні дані (задані неповно і неточно), що дозволяє вирішити задачу з необхідною точністю. Для пояснення ідеї зупинимося на короткому описі алгоритму функціонування блокчейн при використанні технології угоди

«Proof-of-works», зручне для подальшого аналізу.

1. Алгоритм забезпечення цілісності інформації. Для забезпечення цілісності використовується результат обчислення хеш-коду по методу двійкового дерева Меркле [7, с. 40-45] (рис. 2.3). Таким чином, для верифікації цілісності і -го блоку даних рівнях ієрархії і «корінь хеш-дерева», тобто кортеж

$$\langle (h_n^i, h_n^{i+1}), (h_{n-1}^i, h_{n-1}^{i+1}), \dots, (h_1^i, h_1^{i+1}), h_0 \rangle$$

Всього для верифікації блоку даних необхідно не більше $O(\log_2 n)$ операцій та хеш-кодів. Загальний принцип побудови конструкції «ланцюжка блоків транзакцій» - blockchain показаний на рис.2.3.



Риунок 2.3 – Загальний принцип побудови конструкції «Ланцюжка блоків транзакцій» - blockchain

2. Алгоритм додавання нового блоку в блокчейн при застосуванні протоколу угоди «proof-of-works».

2.1. Нові транзакції отримують всі учасники протоколу угоди.

2.2. Всі учасники протоколу угоди генерують блок транзакцій за певними правилами (наприклад, генерують і перевіряють правильність побудови дерева Меркля і цифрові підписи кожної транзакції).

2.3. Всі учасники протоколу формують «цифрову пломбу» блоку шляхом вирішення обчислювально складної задачі. Відомим прикладом такого завдання є обчислення хеш-коду від заданих даних (так званої «хеш-головоломки»), а саме завдання знайти таке значення nonce. Відомо що для сильної хеш-функції ця задача вирішується тільки методом прямого перебору за всіма значеннями nonce.

2.4. Учасники протоколу перевіряють цифрову пломбу учасника, який сформував її раніше за всіх і при правильності перевірки додають цей блок в ланцюжок блоку транзакцій.

Алгоритм угоди на підставі «доказу точності ». Для вирішення проблем протоколів узгодження, викладених вище, пропонується змінити обчислення функції формування «Цифровий пломби» (пункт 2.3 алгоритму додавання нового блоку в блокчейн при застосуванні протоколу угоди «proof-of-works») таким чином, щоб необхідні вхідні дані були задані неповно і неточно, а значення функції потрібно обчислити з точністю, що задається деяким порогом. Інформація про вхідні дані розташовується на декількох ресурсах за доступ до яких конкурують учасники протоколу угоди. Остання властивість дозволяє зрівнювати шанси учасників протоколу з високопродуктивними і малопродуктивними обчислювальними ресурсами в боротьбі за право генерації нового блоку.

Фундаментальною частиною біткоїнів є криптографічні алгоритми. Зокрема, алгоритм ECDSA – Elliptic Curve Digital Signature Algorithm, який використовує еліптичні криві (elliptic curve) і кінцеві поля (finite field) для підпису даних, щоб третя сторона могла підтвердити автентичність підпису, виключивши можливість її підробки. У ECDSA для підпису і верифікації використовуються різні процедури, що складаються з декількох арифметичних операцій.

Еліптична крива над полем K – це кубічна крива над алгебраїчним замиканням поля K, що задається рівнянням третього ступеня з коефіцієнтами з поля K і «точкою на нескінченності». Однією з форм еліптичних кривих є криві Вейерштрасса.

$$y^2 = x^3 + ax + b \qquad (2.1)$$

Для коефіцієнтів a = 0 і b = 7 (використовуваних в біткоїнах), графік функції приймає наступний вигляд:

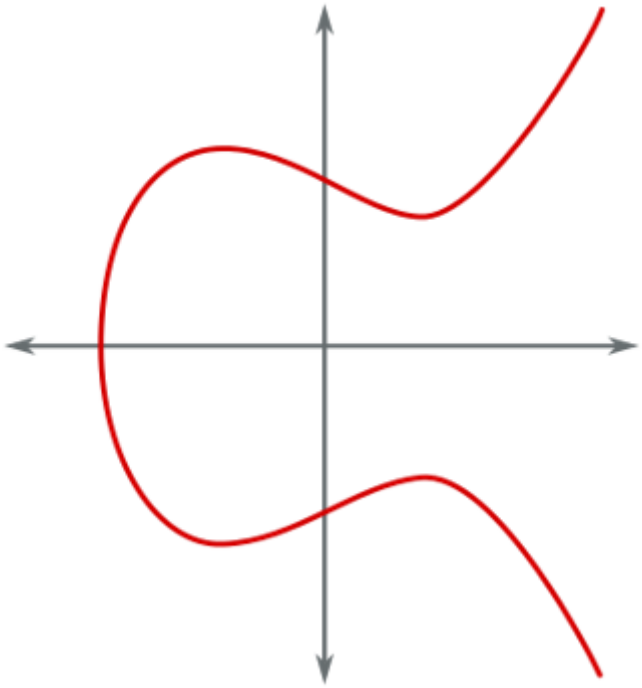


Рисунок 2.4 – Еліптична крива

Еліптичні криві мають кілька цікавих властивостей, наприклад, невертикальна лінія, яка перетинає дві точки на кривій, перетне третю точку на кривій. Сумою двох точок на кривій P + Q називається точка R, яка є відображенням точки -R (побудованої шляхом продовження прямої (P, Q) до перетину з кривою) щодо осі X.

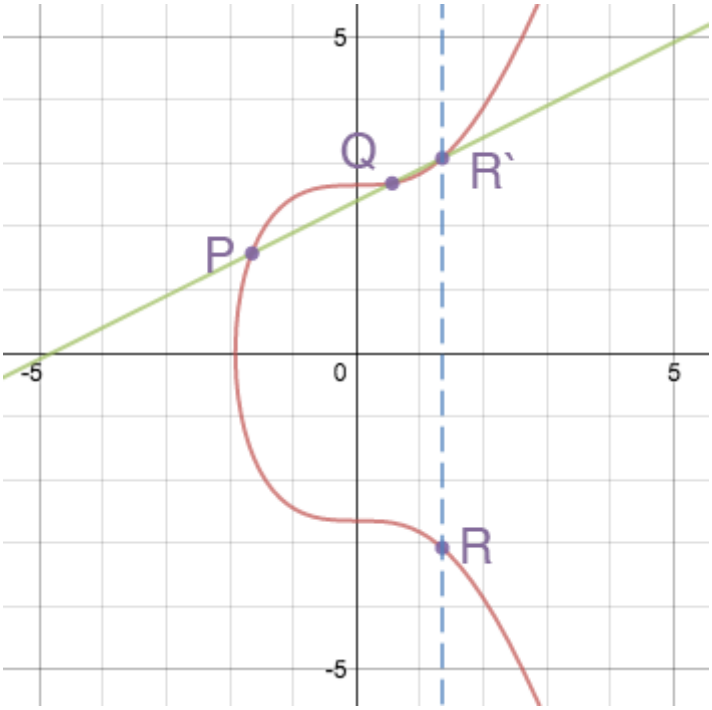


Рисунок 2.5 – Сума двох точок на кривій

Якщо ж провести пряму через дві точки, що мають координати виду P (a, b) і Q (a, -b), то вона буде паралельна осі ординат. У цьому випадку не буде третьої точки перетину. Щоб вирішити цю проблему, вводиться так звана точка на нескінченності (point of infinity), що позначається як O. Тому, якщо перетин відсутній, рівняння приймає наступний вигляд P + Q = O.

Якщо необхідно скласти точку саму з собою (подвоїти її), то в цьому випадку просто проводиться дотична до точки Q. Отримана точка перетину відбивається симетрично щодо осі X.

Ці операції дозволяють провести скалярне множення точки R = k * P, складаючи точку P саму з собою k раз. Однак зазначимо, що для роботи з великими числами використовуються більш швидкі методи.

Еліптична крива над кінцевим полем

В еліптичній криптографії (ECC) використовується така ж крива, тільки розглянута над деяким кінцевим полем. Кінцеве поле в контексті ECC можна уявити як визначений набір позитивних чисел, в якому повинен надаватися результат кожного обчислення.

$$y^2 = x^3 + ax + b \pmod p \qquad (2.2)$$

Наприклад, 9 mod 7 = 2. Тут маємо кінцеве поле від 0 до 6, і всі операції по модулю 7, над якою цифрою вони б не здійснювалися, дадуть результат, який потрапляє в цей діапазон.

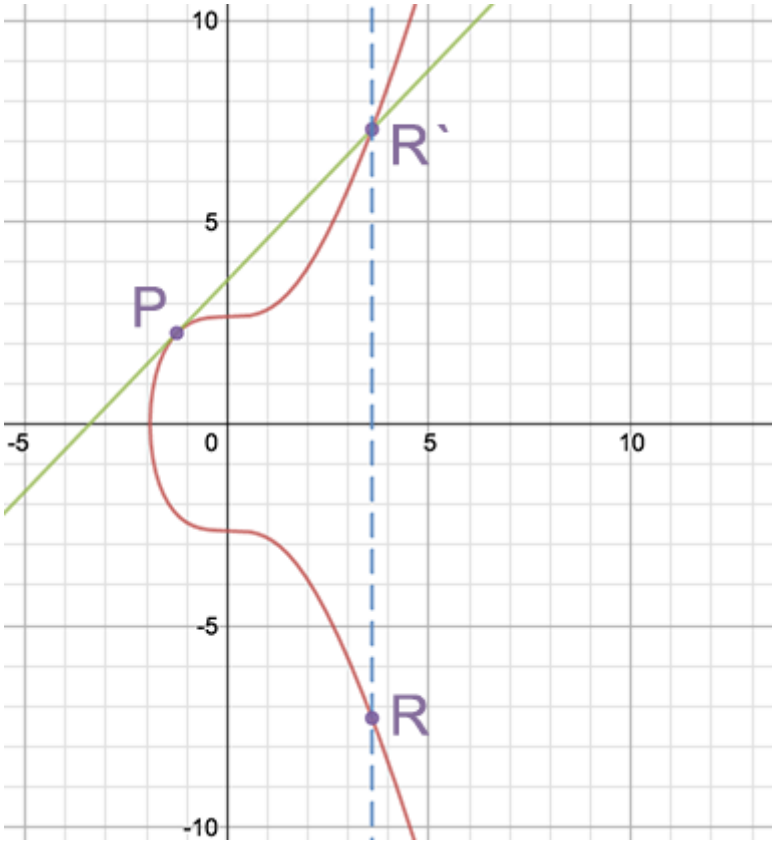


Рисунок 2.6 – Подвоєння точки

Всі названі вище властивості (додавання, множення, точка в нескінченності) для такої функції залишаються в силі, хоча графік цієї кривої не буде схожа на еліптичну криву. Еліптична крива біткоїнов, $y^2 = x^3 + 7$, певна на кінцевому полі по модулю 67, виглядає наступним чином:

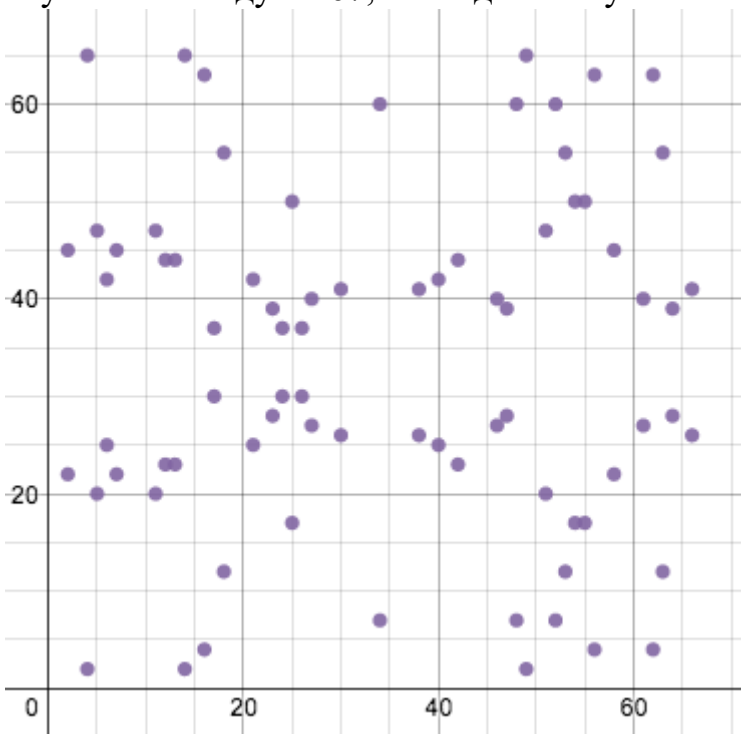


Рисунок 2.7 – Еліптична крива біткоїнів, певна на кінцевому полі по модулю 67

Це безліч точок, в яких всі значення x і y є цілі числа між 0 і 66. Прямі лінії, намальовані на цьому графіку, тепер будуть як би «обертатися» навколо поля, як тільки досягнуть бар'єру 67, і продовжаться з іншого його кінця , зберігаючи колишній нахил, але зі зрушенням. Наприклад, додавання точок (2, 22) і (6, 25) в цьому конкретному випадку виглядає так:

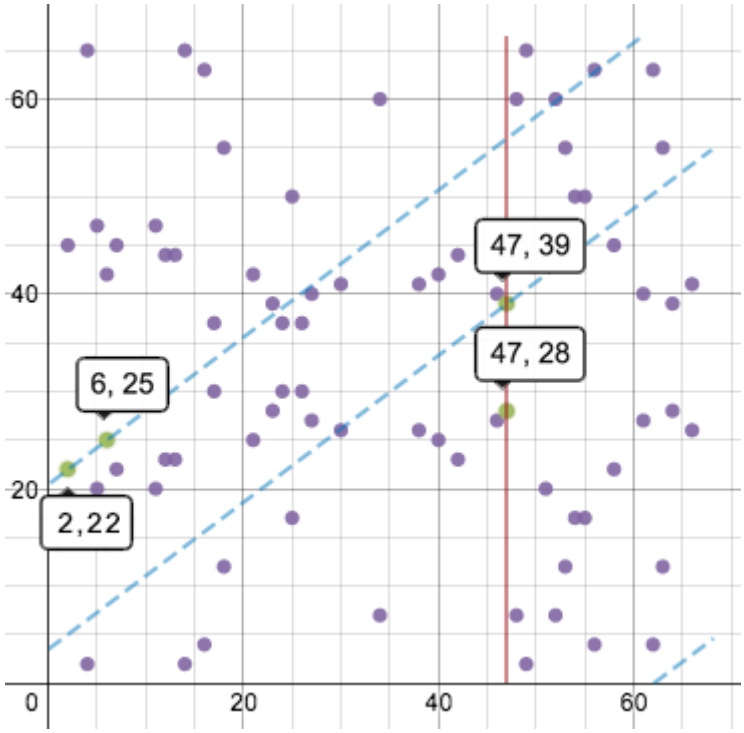


Рисунок 2.8 – Додавання точок (2, 22) і (6, 25)

У протоколі біткоїнів зафіксований набір параметрів для еліптичної кривої і її кінцевого поля, щоб кожен користувач використовував строго певний набір рівнянь. Серед зафіксованих параметрів виділяють рівняння кривої (equation), значення модуля поля (prime modulo), базову точку на кривій (base point) і порядок базової точки (order). Цей параметр підбирається спеціально і є дуже великим простим числом.

У разі біткоїнів використовуються наступні значення:

Рівняння еліптичної кривої: $y^2 = x^3 + 7$

Простий модуль:

2 256 - 2 32 - 2 9 - 2 8 - 2 7 - 2 6 - 2 4 - 1 = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F

Базова точка:

04 **79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798** 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

Жирним шрифтом виділено координата X в шістнадцятковому записі. За нею відразу слідує координата Y.

Порядок: FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

Цей набір параметрів для еліптичної кривої відомий як secp256k1 і є частиною сімейства стандартів SEC (Standards for Efficient Cryptography), пропонованих для використання в криптографії. У біткоїнів крива secp256k1 використовується спільно з алгоритмом цифрового підпису ECDSA (elliptic curve digital signature algorithm). У ECDSA секретний ключ – це випадкове число між одиницею і значенням порядку. Відкритий ключ формується на підставі секретного: останній множиться на значення базової точки. Рівняння має наступний вигляд:

Відкритий ключ = секретний ключ * G

Це показує, що максимальна кількість секретних ключів (отже, біткоїн-адреса) - звичайна, і дорівнює порядку. Однак порядок є неймовірно великим числом, так що випадково або навмисно підібрати секретний ключ іншого користувача нереально.

Обчислення відкритого ключа виконується за допомогою тих же операцій подвоєння і складання точок. Це тривіальна задача, яку звичайний персональний комп'ютер або смартфон вирішує за мілісекунди. А ось зворотна задача (отримання секретного ключа з публічного) - є проблемою дискретного логарифмування , яка вважається обчислювально складною (хоча суворого доказу цього факту немає). Кращі відомі алгоритми її вирішення, мають експонентну складність. Для secp256k1, щоб вирішити задачу, потрібно близько 2 128 операцій, що потребують часу обчислення на звичайному комп'ютері, порівнянного з часом існування Всесвіту.

Коли пара секретний / публічний ключ отримана, її можна використовувати для підпису даних. Ці дані можуть бути будь-якої довжини. Зазвичай першим кроком виконується хешування даних з метою отримання унікального значення з числом бітів, рівним бітності порядку кривої (256). Після хешування, алгоритм підпису даних z виглядає наступним чином. Тут, G - базова точка, n - порядок, a d - секретний ключ.

Вибирається деяке ціле k в межах від 1 до n-1

Розраховується точка (x, y) = k * G з використанням скалярного множення

Знаходиться r = x mod n. Якщо r = 0, то повернення до кроку 1

Знаходиться s = (z + r * d) / k mod n. Якщо s = 0, то повернення до кроку 1

Отримана пара (r, s) є підписом

Після отримання даних і підписів до них, третя сторона, знаючи публічний ключ, може їх верифікувати. Кроки для перевірки підпису такі (Q - відкритий ключ):

Перевірка, що і r, і s перебувають в діапазоні від 1 до n-1

Розраховується w = s -1 mod n

Розраховується u = z * w mod n

Розраховується v = r * w mod n

Розраховується точка (x, y) = uG + vQ

Якщо r = x mod n, то підпис вірна, інакше - недійсна

Справді,

uG + vQ = u + vdG = (u + vd) G = (zs -1 + rds -1) G = (z + rd) s -1 G = kG

Остання рівність використовує визначення s на етапі створення підпису.

Безпека ECDSA пов'язана зі складністю завдання пошуку секретного ключа, описаного вище. Крім цього, безпека вихідної схеми залежить від «випадковості» вибору k при створенні підпису. Якщо одне і те ж значення k використовувати більш ніж один раз, то з підписів можна витягти секретний ключ. Тому сучасні реалізації ECDSA, в тому числі використовувані в більшості біткоїн-гаманців, генерують k детерміновано на основі секретного ключа і підписується повідомлення.

Для перевірки цілісності файлів використано алгоритм MD5.

Алгоритм MD5 є алгоритмом обчислення "хеш-функції" (Message digest) для різних цілей – шифрування паролів, перевірка цілісності файлів, і т.д. На вхід подається потік даних довільної довжини, а на виході отримуємо хеш довжиною 128 біт. Сила цього алгоритму полягає в тому, що практично дуже складно, майже неможливо, знайти два рядки, що дають однаковий хеш. Однак, при певних умовах, можливо отримання початкового тексту. Але цей метод заснований на певному виборі початкових значень, тому не представляє практичної цінності. Також MD5 алгоритм використовується в додатках криптографії та електронно-цифрових підписів для генерації ключа шифрування.

При розробці даного алгоритму бралася до уваги швидкість роботи на сучасних 32-розрядних системах, а також вимога мінімізації використовуваної пам'яті. Порівняно з MD4, MD5 повільніший, ніж MD4, але в той же час і більш стійким, в силу особливостей побудови.

Введемо наступні позначення: під "словом" буде матися на увазі кількість інформації в 32 біта, а під "Байтом" - 8 біт. Послідовність біт будемо розглядати як сукупність електронних даних, старший байт йде першим, молодший – останнім. Аналогічно представляється послідовність байт, як послідовність слів, тільки молодший байт йде першим.

На вхід алгоритму подається вхідний потік даних довжиною N.

N може бути довільним цілим невід'ємним числом. Це число може бути як кратним, так і не мати, 8. Процес обчислення MD5 суми складається з декількох кроків. Розглянемо їх докладніше.

Крок 1: вирівнювання потоку.

Процес вирівнювання полягає в дописуванні в кінець потоку 1, а потім деякого числа нулів. нулі додаються до тих пір, поки довжина всього потоку не стане рівною 512 * N + 448, тобто рівною 448 по модулю 512. Таке вирівнювання відбувається в будь-якому випадку, навіть якщо довжина потоку вже задовольняє даній умові.

Таблиця 2.1 – Таблиці істинності для цих функцій:

x	y	z	F
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Таблиця 2.2 – Таблиці істинності для цих функцій:

x	y	z	G
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Таблиця 2.3 – Таблиці істинності для цих функцій:

x	y	z	H
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Таблиця 2.4 – Таблиці істинності для цих функцій:

x	y	z	I
0	0	0	1

0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

Крок 2: додавання довжини.

Потім в кінець дописується двійкове подання довжини початкового потоку-всього 64 біта. Якщо ж довжина більше ніж 2^{64}, то беруться молодші 64 біта. Це додавання представляє собою два «слова», молодше йде першим, за ним старше.

Після цього сумарна довжина потоку стане кратною 16 ^{32} бітовим словами.

Подальше обчислення ґрунтується на уявленні цього розширеного потоку як масиву слів довжини N: A [0, ... N-1].

Крок 3: ініціалізація MD буфера.

При обчисленнях буде використовуватися буфер з 4 слів - A, B, C, D, в якому зберігаються результати проміжних обчислень. Початкові значення, що знаходяться в цьому буфері, наступні:

A = 0x67452301

B = 0xEFCDAB89

C = 0x98BADCFE

D = 0x10325476

Крок 4: обробка потоку блоками по 16 слів.

Для подальших обчислень нам необхідно ввести наступні функції, що залежать від 3 параметрів - «слів». Результатом роботи цих функцій буде також «слово».

F(x, y, z) = (x & y) | (~x & z)

(x, y, z) = (x & z) | (y & ~z)

H(x, y, z) = x ^ y ^ z

I(x, y, z) = y ^ (x | ~z)

Тут «&» позначає побітову операцію «AND», «|» побітову операцію «XOR», «^» операцію побітового «XOR», «~» операцію побітового «NOT»

На цьому етапі також знадобиться таблиця констант T [1 ... 64], заповнена за допомогою наступної формули: T [i] = [4294967296 * abs (sin (i))], де [] є операція взяття цілої частини.

Визначимо також операцію циклічного зсуву слова X на Y:

X <<< Y.

Подальший опис алгоритму, його основна частина, буде написано на псевдокоді.

// розбиваємо потік на блоки по 16 слів:

for i = 0 to N / 16 - 1 do

```
{
 // i-й блок заноситься в X
 for j = 0 to 15 do
 X [j] = M [i * 16 + j]
 // Зберігаємо значення A, B, C, D
 AA = A
 BB = B
 CC = C
 DD = D
 // раунд 1
 // [abcd k s i] позначає операцію
 // a = b + ((a + F (b, c, d) + X [k] + T [i]) <<< s)
 // виконується 16 операцій:
 [ABCD 0 Разом 7 1] [DABC 1 12 2] [CDAB 2 17 3] [BCDA3 22 4]
 [ABCD 4 7 5] [DABC 5 12 6] [CDAB 6 17 7] [BCDA7 22 8]
 [ABCD 8 7 9] [DABC 9 12 10] [CDAB 10 17 11] [BCDA11 22 12]
 [ABCD 12 7 13] [DABC 13 12 14] [CDAB 14 17 15] [BCDA15 22 16]
 // раунд 2
 // [abcd k s i] позначає операцію
 // a = b + ((a + G (b, c, d) + X [k] + T [i]) <<<
s)
 // виконується 16 операцій:
 [ABCD 1 5 17] [DABC 6 9 18] [CDAB 11 14 19] [BCDA 0 20 20]
 [ABCD 5 5 21] [DABC 10 9 22] [CDAB 15 14 23] [BCDA 4 20 24]
 [ABCD 9 5 25] [DABC 14 9 26] [CDAB 3 14 27] [BCDA 8 20 28]
 [ABCD 13 5 29] [DABC 2 9 30] [CDAB 7 14 31] [BCDA 12 20 32]
 // раунд 3
 // [abcd k s i] позначає операцію
 // a = b + ((a + H (b, c, d) + X [k] + T [i]) <<< s)
 // виконується 16 операцій:
 [ABCD 5 4 33] [DABC 8 11 34] [CDAB 11 16 35] [BCDA 14 23 36]
 [ABCD 1 4 37] [DABC 4 11 38] [CDAB 7 16 39] [BCDA 10 23 40]
 [ABCD 13 4 41] [DABC 0 11 42] [CDAB 3 16 43] [BCDA 6 23 44]
 [ABCD 9 4 45] [DABC 12 11 46] [CDAB 15 16 47] [BCDA 2 23 48]
 // раунд 4
 // [abcd k s i] позначає операцію
 // a = b + ((a + I (b, c, d) + X [k] + T [i]) <<< s)
 // виконується 16 операцій:
 [ABCD 0 6 49] [DABC 7 10 50] [CDAB 14 15 51] [BCDA 5 21 52]
 [ABCD 12 6 53] [DABC 3 10 54] [CDAB 10 15 55] [BCDA 1 21 56]
 [ABCD 8 6 57] [DABC 15 10 58] [CDAB 6 15 59] [BCDA 13 21 60]
 [ABCD 4 6 61] [DABC 11 10 62] [CDAB 2 15 63] [BCDA 9 21 64]
 A + = AA
 B + = BB
```

```
C + = CC
D + = DD
}
```

Крок 5: висновок MD5.

Остаточний результат, що знаходиться в буфері A-D, і є майже готовий хеш. Виводячи «слова» з цього буфера в зворотному порядку, отримаємо готовий хеш. Тобто md5hash = DCBA.

Наступний список являє собою різницю між MD4 і MD5:

1. MD5 має на один раунд більше - 4 проти 3 у MD4.

2. Що б зменшити вплив вхідного тексту була введена унікальна константа для кожного раунду-T [i].

3. У другому раунді замінили функцію g с (XY v XZ v YZ) на (XZ v Y not (Z)), для того, щоб зробити g менш симетричною.

4. На кожному кроці використовується значення, отримане на попередньому кроці. Це дає більш швидку зміну результату при зміні вхідних даних.

5. Для цих же цілей кількість зрушень відрізняється від раунду до раунду, і вибрано так, що б ще більше збільшити цей ефект.

6. Змінено порядок, в якому обробляються слова в раундах 2 і 3, для того щоб зробити їх менш схожими один на одного.

Для того, що б показати різницю в швидкості MD4 і MD5, був проведено наступний експеримент. Результати занесені в таблицю 2.2.

Суть експерименту полягає в тому, що б заміряти час, витрачений на побудову 10000 хеш від повідомлення розміром 10000 байт.

Обчислення проводилися на Intel Pentium III 750 МГц. В двох реалізаціях були обрані реалізація з пакета

OpenSSL і заснована на RFC1321.

Таблиця 2.5 – Порівняння алгоритмів MD4 і MD5

	MD4		MD5	
RFC	2.574 сек	37940 кБ/сек	2.614 сек	37359 кБ/сек
OpenSSL	0.891 сек	109603 кБ/сек	1.152 сек	84771 кБ/сек

Результати дослідження показують, що:

У реалізації RFC MD5 повільніше MD4 на 1.55% .. 4.92%

У реалізації MD5 повільніше MD4 на 29.29% .. 39.82%

Але, тим не менш, в даний час MD5 використовується набагато ширше, ніж MD4. Це пов'язано в першу чергу з підвищеною надійністю першого.

2.3 Архітектура системи документообігу та документообміну за допомогою криптографії та технологіїї blockchain

У рамках реалізації системи документообігу та документообміну за допомогою криптографії та технологіїї blockchain обрано високорівневу мову програмування Python.

Python – високорівнева мова програмування загального призначення, орієнтована на підвищення продуктивності розробника і читання коду. Синтаксис ядра Python мінімалістичний. У той же час стандартна бібліотека включає великий обсяг корисних функцій.

Python підтримує структурне, об'єктно-орієнтоване, функціональне, імперативне і аспектно-орієнтоване програмування. Основні архітектурні риси – динамічна типізація, автоматичне керування пам'яттю, повна інтроспекція, механізм обробки виключень, підтримка багатопоточних обчислень, високорівневі структури даних. Підтримується розбиття програм на модулі, які, в свою чергу, можуть об'єднуватися в пакети.

Еталонної реалізацією Python є інтерпретатор CPython, що підтримує більшість активно використовуваних платформ [11]. Він поширюється під вільною ліцензією Python Software Foundation License, що дозволяє використовувати його без обмежень в будь-яких додатках, включаючи пропрієтарні [12]. Є реалізація інтерпретатора для JVM з можливістю компіляції, CLR, LLVM, інші незалежні реалізації. Проект використовує JIT-компіляцію, яка значно збільшує швидкість виконання Python-програм.

Python - мова програмування, що активно розвивається, нові версії з додаванням / зміною мовних властивостей виходять приблизно раз в два з половиною роки. Язик не піддавався офіційній стандартизації, роль стандарту де-факто виконує CPython, що розробляється під контролем автора мови. На даний момент Python займає третє місце в рейтингу TIOBE з показником 8,5%. Аналітики відзначають, що це найвищий бал Python за весь час його присутності в рейтингу.

Загальна структура модулів наведена на рис. 2.9

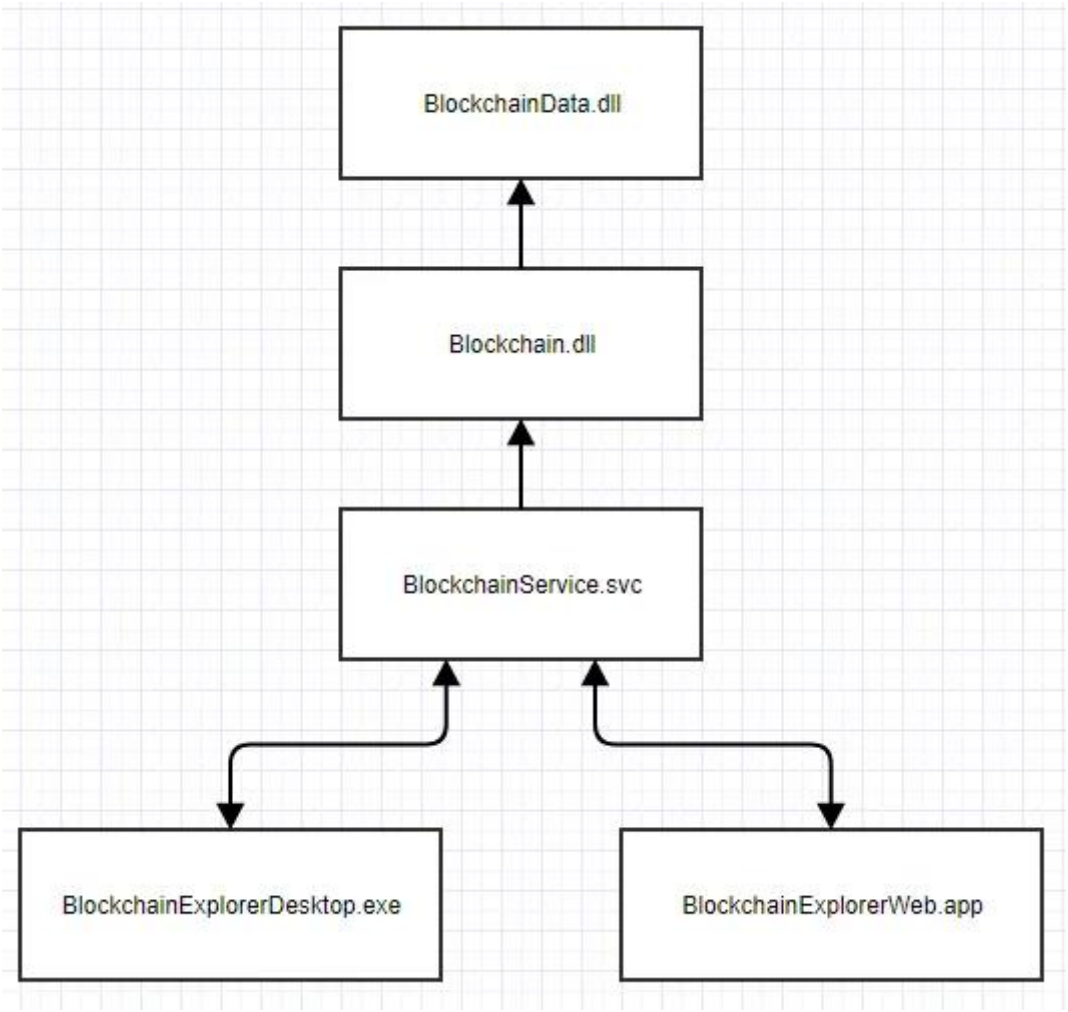


Рисунок 2.9 – Структура модулів блокчеїна

Додаток розділено на кілька проектів.

BlockchainData – рівень даних. Заздалегідь передбачено можливість розширення можливих засобів для збереження даних. В даному випадку використовується єдина реалізація збереження з використанням EntityFramework.

Blockchain – рівень логіки. Тут реалізовані всі основні класи та логіка роботи програми.

BlockchainService – WCF-служба, що надає REST API інтерфейс для клієнтських додатків.

BlockchainExplorerDesktop – WinForms-додаток для перегляду даних, що зберігаються в блокчейн.

BlockchainExplorerWeb – MVC ASP.NET додаток для перегляду даних, що зберігаються в блокчейн.

Розглянемо докладніше реалізацію основної бібліотеки класів Blockchain.dll.

Отже, основним класом бібліотеки є клас Chain.cs. Він взаємодіє з рівнем даних використовуючи принципи інверсії управління і впровадження залежностей.

Таким же чином реалізований підхід до алгоритму хешування. Chain містить в собі список всіх блоків в сховище даних, а також підсписки для поділу блоків за типами (блоки даних, блоки з даними про користувачів, блоки з даними про IP адреси серверів). При створенні екземпляра класу ланцюжка блоків виконується звернення до глобальної мережі для синхронізації з іншими хостами. Також виконується отримання блоків з локального сховища. На даний момент не реалізовано коректного алгоритму злиття цих двох ланцюжків. Вибирається просто в найбільш довгий ланцюг. Якщо не було отримано ні локального, ні глобального ланцюжка, то виконується створення нового ланцюжка, який складається з одного генезис-блоку. Функціональна модель блокчеїн наведена на рис. А.1, додаток А.

Генезис блок – це єдиний початковий блок ланцюжка. Він завжди генерується за однаковими правилами у всіх примірників блокчеїн. Після створення екземпляра ланцюжка виконується його повна перевірка на коректність, щоб упевнитися, що не було внесено жодних змін.

Інверсія управління (Inversion of Control, IoC) це певний набір рекомендацій, що дозволяють проектувати і реалізовувати програми використовуючи слабке зв'язування окремих компонентів. Тобто, для того щоб слідувати принципам інверсії управління необхідно:

- Реалізовувати компоненти, що відповідають за одну конкретну задачу;
- Компоненти повинні бути максимально незалежними один від одного;
- Компоненти не повинні залежати від конкретної реалізації один одного.

Одним з видів конкретної реалізації даних рекомендацій є механізм Впровадження залежностей (Dependency Injection, DI). Він визначає дві основні рекомендації:

- модулі верхніх рівнів не повинні залежати від модулів нижніх рівнів. Обидва типи модулів повинні залежати від абстракцій;
- абстракції не повинні залежати від деталей. Деталі повинні залежати від абстракцій.

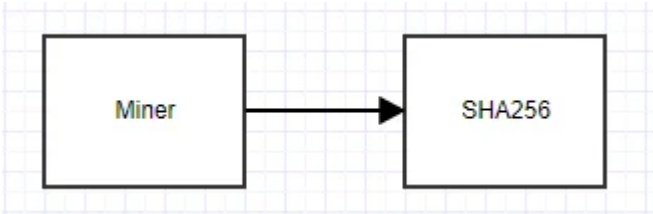


Рисунок 2.10– Зв'язок між класами

Тобто, якщо у будуть існувати два пов'язаних класи, то необхідно реалізовувати зв'язок між ними не безпосередньо, а через інтерфейс. Це дозволить при необхідності динамічно міняти реалізацію залежних класів.

Будь-яка криптовалюта заснована на будь-якій хеш-функції (алгоритмі). Припустимо, що програма буде виконувати обчислення на алгоритмі SHA256, для Майнінг біткоїни. Тоді отримаємо такий зв'язок між класами:

Проблема полягає в тому, що в даний час алгоритмів, на яких засновані крипто валюти досить багато і їх число постійно збільшується. Якщо необхідно додати нові алгоритми для Майнінг інших крипто валют, доведеться вносити велику кількість змін в сам клас Майнера. Щоб цього уникнути, необхідно створити проміжний інтерфейс, від якого буде залежати майнер і який повинні будуть реалізовувати різні алгоритми.

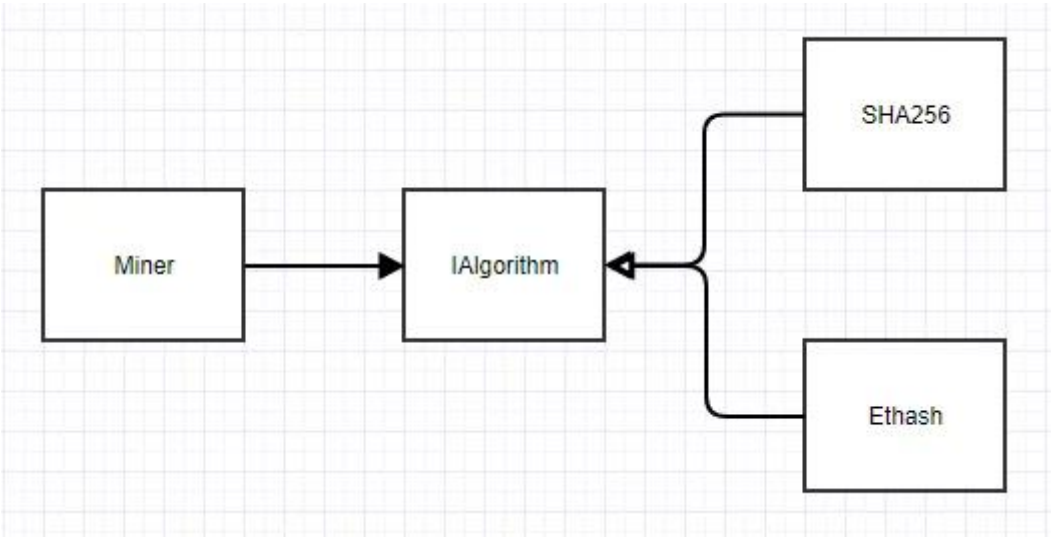


Рисунок 2.11 – Реалізація зв’язку

Так є можливість не тільки розділити відповідальність за виконання конкретних завдань між класом Майнер і алгоритмами, а й зробити заділ на подальше збільшення кількості підтримуваних алгоритмів.

Існує кілька конкретних патернів впровадження залежностей:

Через конструктор (Constructor injection);

Через властивість класу (Setter injection);

Через аргумент методу (Method injection).

Реалізація блоку ланцюжка Block

Клас блок реалізує структуру блоку даних. Він містить в собі всі необхідні поля, які повинні бути збережені в сховище даних. При створенні блоку виконується хешування вхідних даних, а також змішування всього блоку, що дозволяє гарантувати незмінність збережених даних і метаданих. При виконанні хешування враховуються такі поля: версія, час створення блоку, хеш попереднього блоку, хеш збережених даних, хеш користувача. Результат зберігається в полі Hash блоку, що дозволяє легко перевірити його коректність.

Реалізація класу Збереження даних Data

Клас Даних необхідній для зручності роботи. Він дозволяє зберігати строкові дані, отримувати хеш Збереження даних, а також розділяти

збережені дані по тип (дані про користувачів, дані про сервери, прості збережені текстові дані). Для коректного Збереження контенту виконується серіалізація і десеріалізація в json формат.

Серіалізація – це процес перетворення об'єкта в потік байтів, десеріалізація - це зворотній процес, що дозволяє сформувати з потоку байтів готовий об'єкт. Якщо сформувати це більш простою мовою, виконується збереження всіх значень об'єкта в спеціалізованому тестовому форматі json.

Інтерфейси IHashable і IAlgorithm

Важливою особливістю даної реалізації є використання спеціального інтерфейсу IHashable, який повинен реалізовувати всі класи, які піддаються хешуванню (такі як Block, User, Data). Цей інтерфейс реалізує всього одну властивість і один метод. Властивість строкова Hash гарантує, що у класа буде поле, в яке буде виконано збереження готового хешу об'єкта, а метод GetStringForHash повертає рядок, в якій зберігаються всі тестові дані, важливі для хешування.

Даний інтерфейс використовується в іншому інтерфейсі IAlgorithm. Даний інтерфейс використовується для того, щоб надати можливість подальшого розширення можливостей застосування, шляхом легкого додавання додаткових алгоритмів хешування. Даний інтерфейс визначає один перевантажений метод GetHash, який повертає або хеш стоки, або хеш класи, що реалізовує інтерфейс IHashable.

В даний момент реалізований один алгоритм хешування Sha256 у відповідному класі.

Для коректності роботи класів, що реалізують дані інтерфейси використовується проектування за контрактом. Це дозволяє задати передумови і постумови для всіх класів, які реалізують дані інтерфейси. Завдяки цьому гарантується мінімальна перевірка параметрів у всіх спадкоємців.

Рівень даних BlockchainData

Для зберігання всіх даних програми використовується окремий проект. Це зроблено з метою можливості подальшого розширення можливостей системи для збереження даних в будь-яких системах (текстові файли, різні реляційні і не реляційні бази даних і так далі). Для цього запроваджено спеціальний інтефейс IDataProvider, який визначає набір збережених полів, а також методи додавання нових даних, отримання всіх даних і очищення всього сховища.

Основним серверним контролером системи є WCF служба. Саме вона використовує логіку реалізовану в бібліотеці класів Blockchain. Вона надає кілька REST API інтерфейсів, до яких звертаються клієнтські програми. Запити виконуються в асинхронному режимі, що покращує продуктивність системи. На даний момент реалізована передача даних через GET, що не дуже правильно, але зручно при налагодженні програми.

Створення реєстру результатів інтелектуальної діяльності на основі платформи блокчейн створить можливість легального використання

контенту. Разом з тим перед введенням подібного реєстру необхідно розробити критерії його створення, забезпечити технічне тестування, дотримання балансу інтересів правовласників і користувачів. Особливо актуальним є створення таких реєстрів є в зв'язку з стрімким розвитком соціальних мереж (Instagram, Вконтакте, Facebook, Однокласники), в яких постійно відбувається обмін будь-якими файлами. Тим самим необхідно уважно розглянути питання про створення реєстру на основі технологій блокчейн, в рамках якого користувачі повинні отримати можливість легального використання результатів інтелектуальної діяльності, а правовласники – отримувати винагороду за таке використання [6, 18].

Підприємництво життєво важливо для розвитку економіки і процвітання суспільства. Інтернет повинен був звільнити підприємців, надавши їм кошти і можливості великих компаній, але не їхні проблеми, такі як успадкована культура, робочі процеси і важкий баласт минулого. Однак гучні успіхи доткомів, які зробили своїх власників мільярдерами, маскують неприємну істину: у багатьох розвинених економіках підприємництво і поява нових компаній в останні тридцять років переживають спад [11]. У країнах, що розвиваються Інтернет майже не знизив бар'єри для потенційних підприємців, які змушені боротися з убивчими державними бюрократіями.

Інтернет не дав і мільярдам людей доступу до фінансових інструментів, необхідним для започаткування власної справи. Звісно, не кожному судилося стати підприємцем, але навіть середньостатистичній людині, намагається гідно заробляти, заважають відсутність фінансових інструментів і засилля державних обмежень.

Це складна проблема, але блокчейн багато в чому здатний дати потужний заряд енергії підприємництву і, відповідно, успіху. Тепер, щоб придбати значимість і можливість вести ділову активність за межами своєї спільноти, пересічному громадянинові країни, що розвивається необхідно тільки пристрій, підключений до Інтернету. Доступ до глобальної економіки означає більшу доступність джерел кредитування і фінансування, постачальників, партнерів і можливостей для інвестування. Будь талант, будь-який ресурс, навіть найскромніший, можна монетизувати на блокчейні [8].

За рахунок виключення посередників разом з їх комісійними крипто валюта дозволяє скоротити витрати на ведення бізнесу, а також запобігає корупції, існувала в посередницьких структурах і серед політиків, залучених в орбіту їх діяльності.

Висновки до розділу

У межах другого розділу здійснено розкриття методичних аспектів проектування системи документообігу та документообміну за допомогою криптографії та технологіїї blockchain. Алгоритм реалізації системи документообігу та документообміну за допомогою криптографії та технології

blockchain будується на формуванні блоків з даних, що вводяться. В даному блоці міститься додаткова службова інформація, яка необхідна для забезпечення цілісності і незмінності введених даних, а також для роботи самого ланцюжка блоків. При створенні блоку даних виконується хешування введених даних. Потім виконується хешування всіх збережених даних блоку, після чого цей результат записується в поле Hash. Даний підхід дозволяє гарантувати збереження даних, тому що при зміні будь-якого з полів блоку хоча б на один символ хеш функція поверне зовсім інший результат, і система легко зможе це визначити, виконавши повторне хешування блоку і порівнявши зі збереженим хешем. При цьому кожен блок залежить від хешу попереднього блоку, в результаті чого при зміні будь-якого блоку в ланцюжку, весь ланцюжок стає некоректним. Хешування – це процес перетворення вхідних даних довільної довжини в значення певного формату, шляхом перетворення за заданим алгоритмом. Основна особливість хеш-функції це можливість легкого перетворення вхідних даних в хеш, і неможливість однозначного відновлення вихідних даних з хешу.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ДОКУМЕНТООБІГУ ТА ДОКУМЕНТООБМІНУ НА ПРИВАТНОМУ ПІДПРИЄМСТІ ЗА ДОПОМОГОЮ КРИПТОГРАФІЇ ТА ТЕХНОЛОГІЇ BLOCKCHAIN

3.1 Структура системи документообігу та документообміну за допомогою криптографії та технології blockchain

Структура системи документообігу та документообміну за допомогою криптографії та технології blockchain складається з модулів, робота яких описується у програмного продукті.

Формування блоків здійснюється наступною процедурою:

```
def write_block(name, to_whom, p_hash):
    p_hash = get_hash()
    data = {'name': name,
            'to_whom': to_whom,
            'p_hash': p_hash
    with open(BlockChain_dir + a, 'w') as file:
        json.dump(data, file, indent=4, ensure_ascii=False)
```

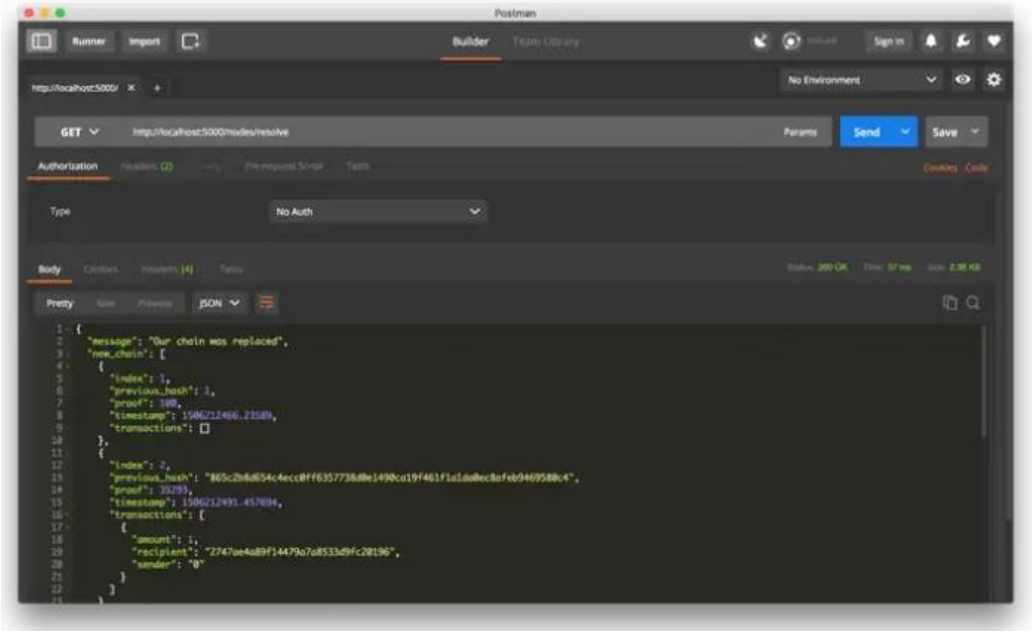


Рисунок 3.1 – Формування блоку

Відкрити утворений блок можно процедурою:

```
with open(BlockChain_dir + a, 'w') as file:
        json.dump(data, file, indent=4, ensure_ascii=False)
```

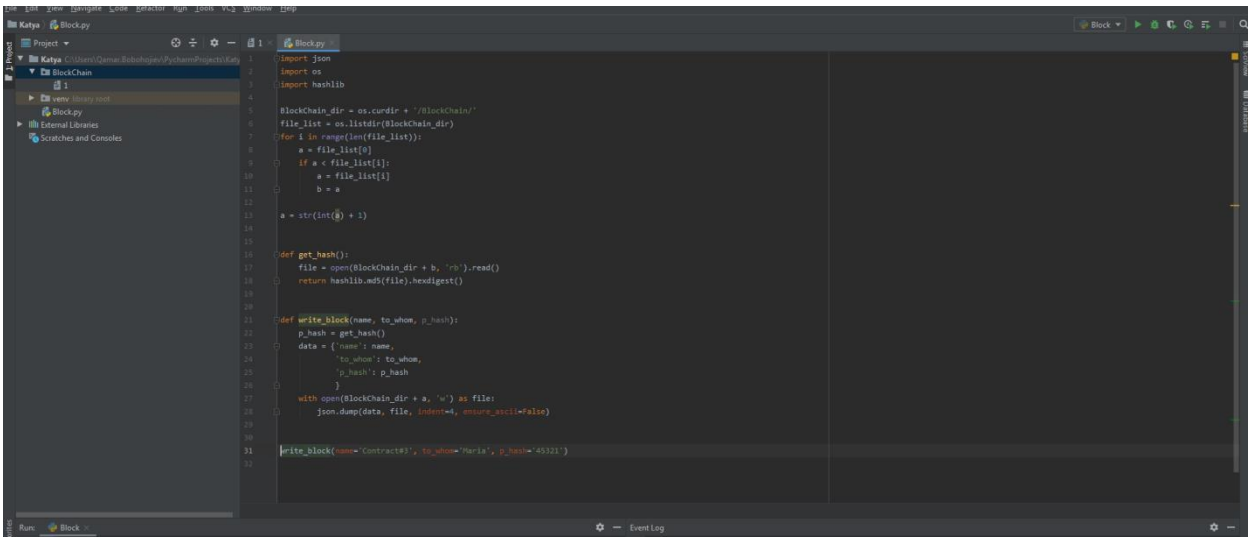


Рисунок 3.2 – Передача блоку

Перехід по ланцюгу блоків здійснюється:

```
BlockChain_dir = os.curdir + '/BlockChain/'
file_list = os.listdir(BlockChain_dir)
for i in range(len(file_list)):
    a = file_list[0]
    if a < file_list[i]:
        a = file_list[i]
        b = a
a = str(int(a) + 1)
```

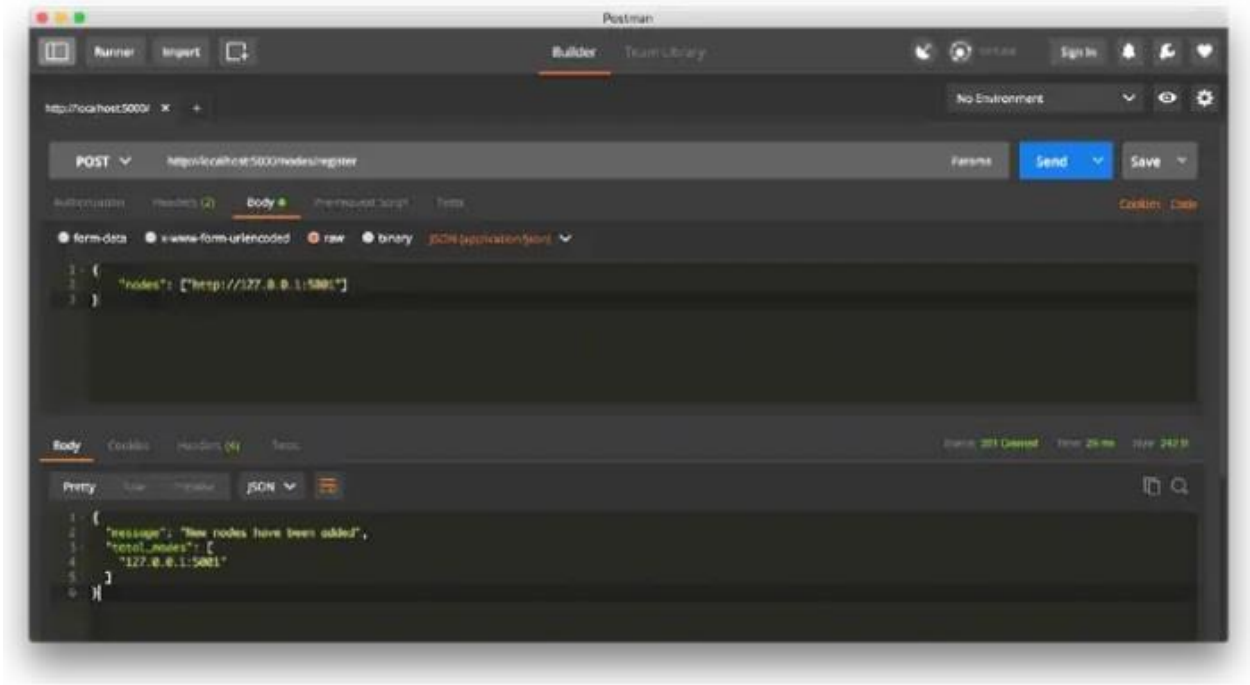


Рисунок 3.3 – Визначення регістру

Скрипт формування потоку

```
import re
import sys
from pkg_resources import load_entry_point

if __name__ == '__main__':
   sys.argv[0] = re.sub(r'(-script\.pyw?|\.exe)?$', '', sys.argv[0])
   sys.exit(
      load_entry_point('pip==19.0.3', 'console_scripts', 'pip')()
```

Передача документу:

```
if ($pyvenvConfigPath) {

      Write-Verbose "File exists, parse `key = value` lines"
      $pyvenvConfigContent = Get-Content -Path $pyvenvConfigPath

      $pyvenvConfigContent | ForEach-Object {
         $keyval = $PSItem -split "\s*=\s*", 2
         if ($keyval[0] -and $keyval[1]) {
            $val = $keyval[1]

            # Remove extraneous quotations around a string value.
            if ("'""".Contains($val.Substring(0,1))) {
               $val = $val.Substring(1, $val.Length - 2)
            }

            $pyvenvConfig[$keyval[0]] = $val
            Write-Verbose "Adding Key: '$($keyval[0])'='$val'"
```

3.2 Тестування системи документообігу та документообміну за допомогою криптографії та технологіїї blockchain

Після написання програми необхідно її протестувати. Для початку створимо черговий блок (рис 3.4, 3.5). У якості блоків в даній реалізації виступає список упорядкованих текстових файлів.

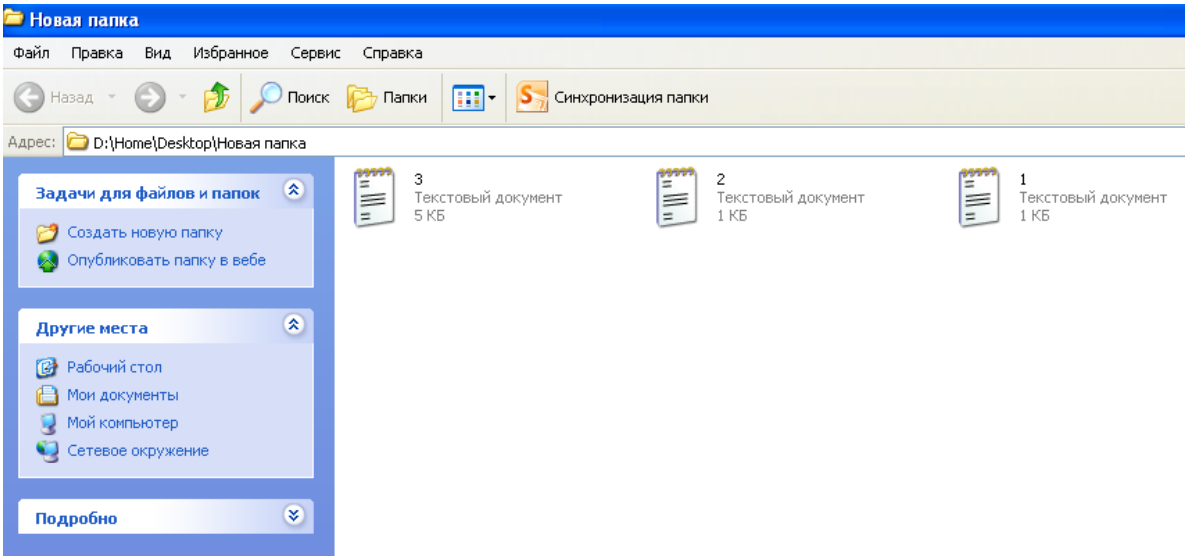


Рисунок 3.4 – Список блоків до додавання

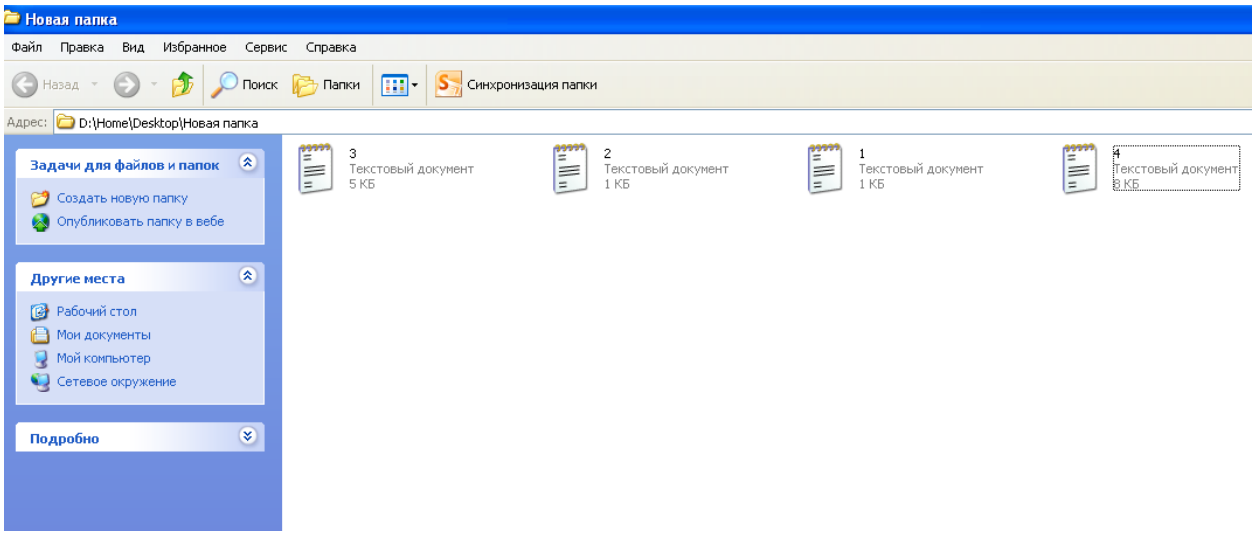


Рисунок 3.5 – Список блоків після створення нового блоку

Внутрішня структура створеного блоку матиме такий вигляд (рис 3.6):

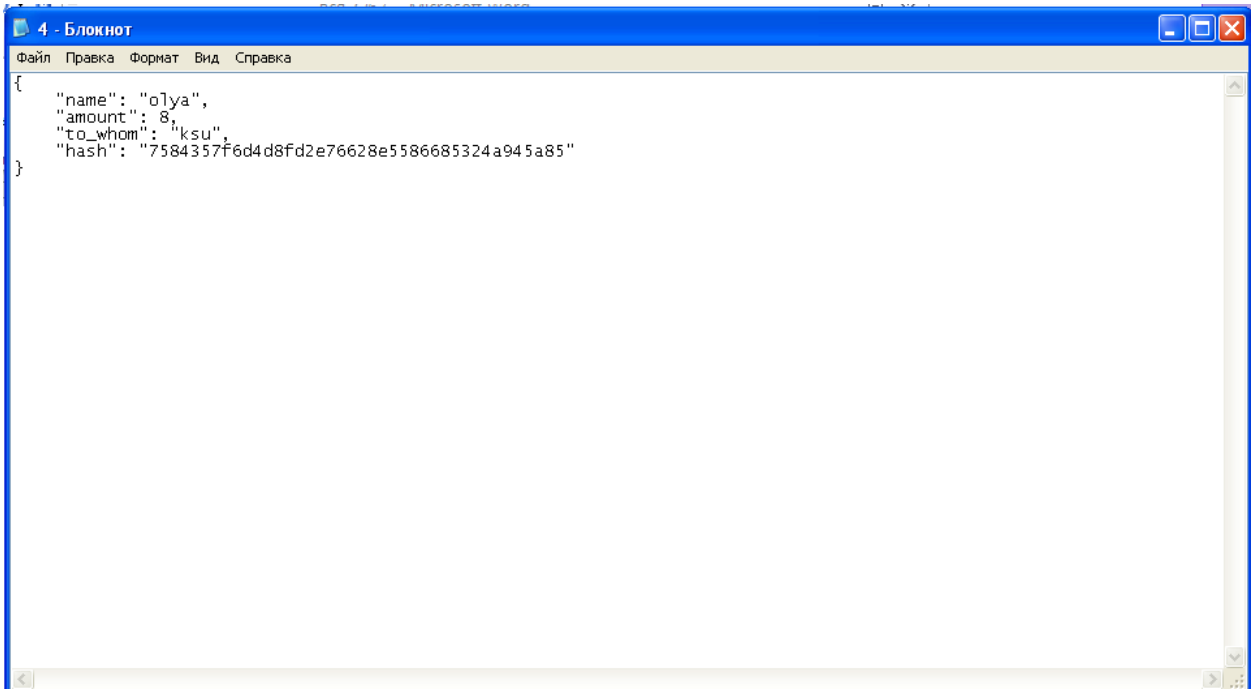


Рисунок 3.6 – Структура створеного блоку

Тепер протестуємо процедуру перевірки на цілісність (рис 3.7). Спочатку вона дає такі результати:

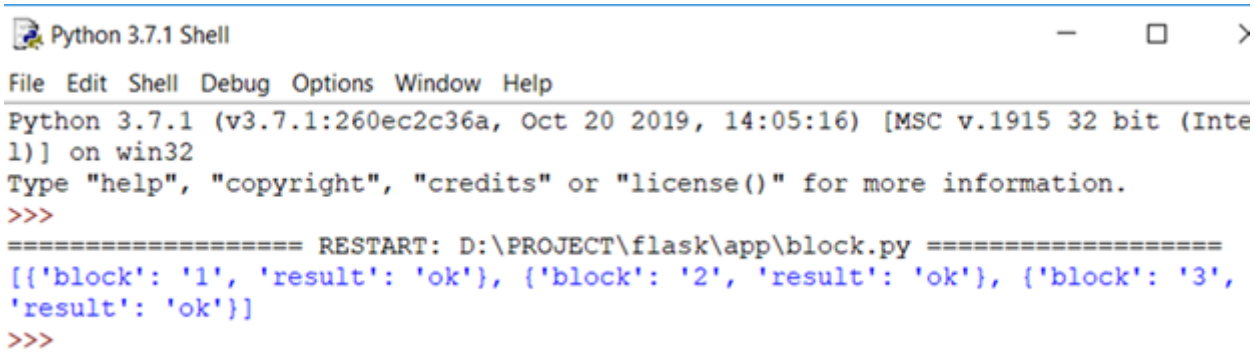


Рисунок 3.7 – Перевірка цілісності блоків

Тобто всі блоки, починаючи з другого (в списку елементи нумеруються починаючи з нуля) успішно проходять перевірку на цілісність.

Тепер спробуємо змінити дані, що містяться в третьому блоці (Рис 3.5). В даному випадку ми змінили суму, що відправляється:

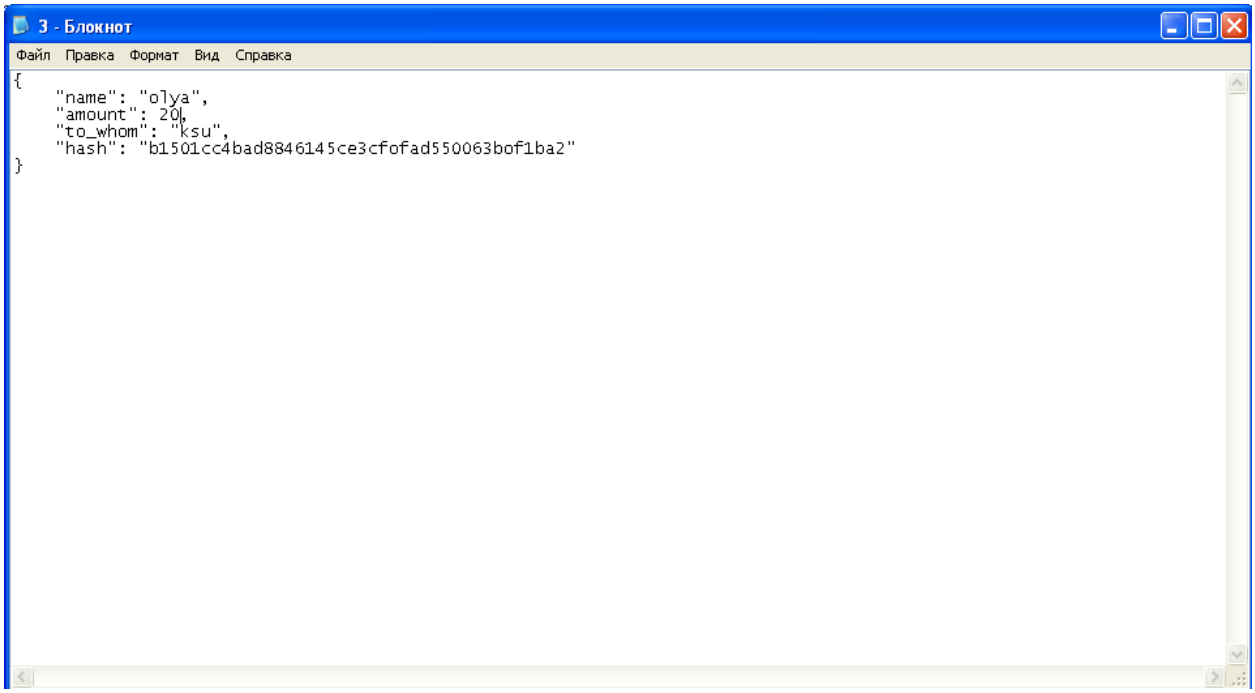


Рисунок 3.8 – Зміна блоку

Перевіримо, який результат тепер видасть перевірка на цілісність (Рис 3.9):

Рисунок 3.9 – Повторна перевірка на цілісність

Тепер ми можемо помітити, що останній з блоків не пройшов перевірку на цілісність, так як ми змінили хеш попереднього блоку.

Таким чином, проведене тестування підтвердило адекватну роботу системи та можливість її впровадження за потребою.

3.3 Верифікація результатів

Проведемо дослідження системи документообігу та документообміну за допомогою криптографії та технології blockchain за показниками діяльності сформуємо табл. 3.1.

Таблиця 3.1 – Значення показників діяльності системи документообігу та документообміну за допомогою криптографії та технологіїї blockchain

Параметр	Значення									
$ПР_1$	1	0	1	1	0	1	1	1	0	1
$ПР_2$	1	0	1	1	0	0	0	1	0	1
$ПР_3$	1	1	1	1	1	1	1	1	1	1
$ПР_4$	1	1	0	0	0	1	0	1	1	0
$КВ_1$	1	2	3	1	3	2	4	1	3	2
$КВ_2$	3	2	4	1	3	2	2	3	4	4
$КВ_3$	2	5	8	8	2	1	5	2	3	5
$КВ_4$	1	2	3	1	3	2	4	1	3	2
$КВ_5$	2	5	8	8	2	5	8	8	7	7
ЗО	9	9	10	10	8	10	8	10	10	9

Відповідно до наведених даних здійснюємо аналіз отриманих даних. Розраховуємо середньоквадратичне відхилення та дисперсію, отримані результати наводимо у таблиці 3.2.

Таблиця 3.2 – Результати математичного аналізу

Параметр	Значення										Середнє відхилення	Дисперсія
$ПР_1$	1	0	1	1	0	1	1	1	0	1	0,42	0,21
$ПР_2$	1	0	1	1	0	0	0	1	0	1	0,5	0,25
$ПР_3$	1	1	1	1	1	1	1	1	1	1	0	0
$ПР_4$	1	1	0	0	0	1	0	1	1	0	0,5	0,25
$КВ_1$	1	2	3	1	3	2	4	1	3	2	0,84	0,96
$КВ_2$	3	2	4	1	3	2	2	3	4	4	0,84	0,96
$КВ_3$	2	5	8	8	2	1	5	2	3	5	2,1	5,69
$КВ_4$	1	2	3	1	3	2	4	1	3	2	0,84	0,96
$КВ_5$	2	5	8	8	2	5	8	8	7	7	2	5,2
ЗО	13	18	29	22	14	15	25	19	22	23	4,2	23,8

Наступним кроком є кореляційний аналіз. Результати у таблиці А.1 додаток А

Аналізуючи дані з табл. 3.3 та використовуючи шкалу Чеддока, можна зробити висновок, що найбільш впливають на ефективність такі чинники:

– $ПР_2$,

- $КВ_1$
- $КВ_2$
- $КВ_4$
- $КВ_5$
- ЗО

На виході цього етапу, згідно до формули:

$$\text{KPI} = \left\{ \bigcup_{w=1}^{v} KPI_w \right\} = \{KPI_1, KPI_2, \dots, KPI_v\}$$

де

$$KPI_w \subseteq KPI, (w = \overline{1, \text{v}})$$

v – кількість ключових показників ефективності.

при w = 6 отримуємо множину ключових показників ефективності KPI :

$$\text{KPI} = \{\text{ПР2}, \text{КВ1}, \text{КВ2}, \text{КВ4}, \text{КВ5}, \text{ЗО}\}$$

Розрахуємо загальну ефективність системи. Показник ефективності CERT:

$$E = {}^{\text{Оцінка}}/_{max} \cdot 100\%$$

Для цього сформуємо таблицю максимальних показників (табл.3.4)

Таблиця 3.4 – Максимальні значення показників

Параметр	Значення
$ПР_1$	1
$ПР_2$	1
$ПР_3$	1
$ПР_4$	1
$КВ_1$	5
$КВ_2$	5
$КВ_3$	10
$КВ_4$	5
$КВ_5$	10
ЗО	39

Наступним кроком розрахуємо ефективності системи документообігу та документообміну за допомогою криптографії та технологіїї blockchain та результати зведемо до таблиці 3.5.

Таблиця 3.5 – Результати розрахунку ефективності

Параметр	Максимальне значення	Оцінка	Ефективність
$ПР_1$	1	0,7	70
$ПР_2$	1	0,5	50
$ПР_3$	1	1	100
$ПР_4$	1	0,5	50
$КВ_1$	5	2,2	44
$КВ_2$	5	2,8	56
$КВ_3$	10	4,1	41
$КВ_4$	5	2,2	44
$КВ_5$	10	6	60
ЗО	39	20	51,28205

Наведемо графічно результати розрахунку:

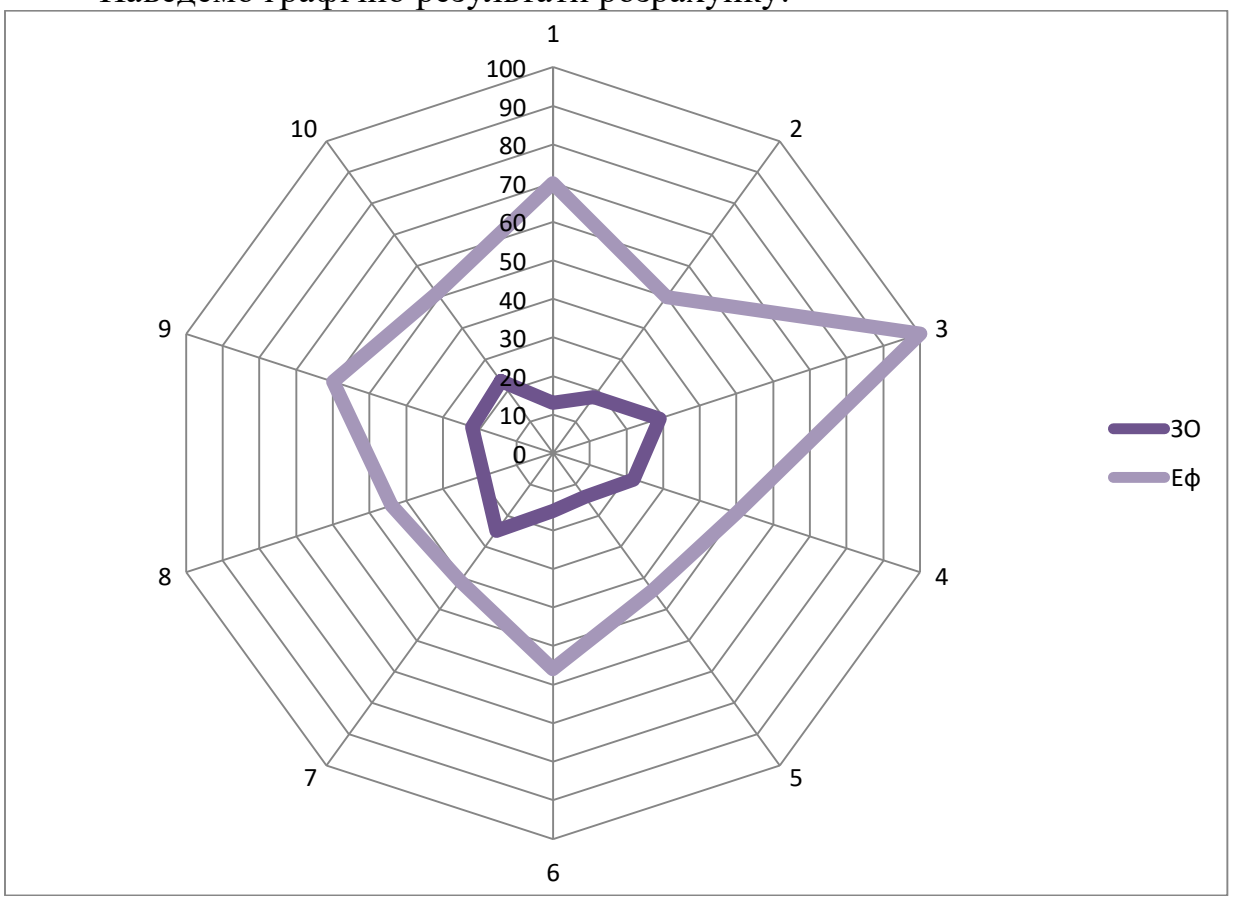


Рисунок 3.10 – Графік залежності ефективності від Загальної оцінки

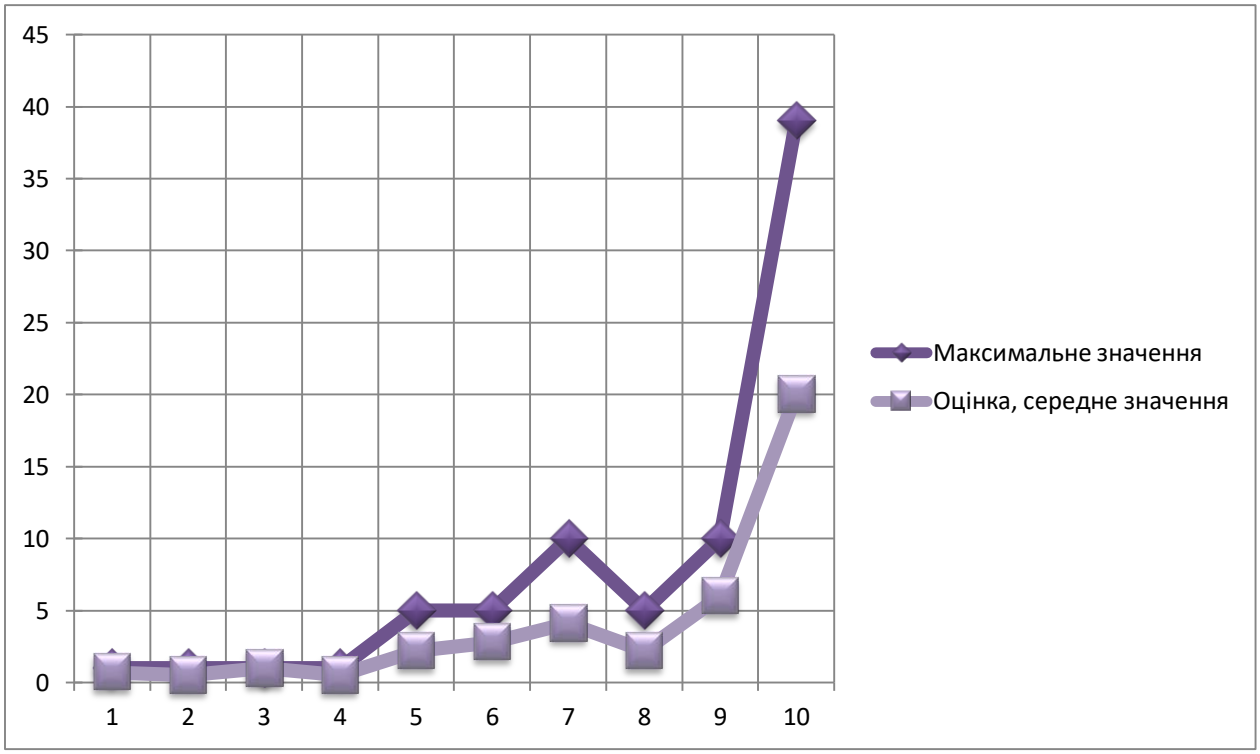


Рисунок 3.11 – Графік залежності ефективності від середньої оцінки

Провівши аналіз отриманих результатів (рис. 3.10 та 3.11), можна зробити висновок про залежність ефективності від кожного із визначених показників.

Висновки до розділу

У межах третього розділу здійснено практичну реалізацію системи документообігу та документообміну на приватному підприємсті за допомогою криптографії та технологіїї blockchain. Проведене тестування підтвердило адекватну роботу системи та можливість її впровадження за потребою.

ВИСНОВКИ

У межах даної роботи здійснено реалізацію системи документообігу та документообміну на приватному підприємсті за допомогою криптографії та технологіїї blockchain. На основі вищевикладеного варто відзначити:

Технологія блокчеїн є універсальним способом зберігання і обробки інформації майже в будь-якій сфері діяльності, що сприяє формуванню нових крипто-інститутів і крипто-індустрій. Вже очевидно, що ця технологія і ті зміни, які вона в собі несе, революційна і призведе до глобальних світових змін. Блокчеїн надасть широкий вплив на фінансові ринки і такі сфери, як платежі, банкінг, розрахунки з цінних паперів, кібербезпека, брокерська звітність, аналіз торгів і прогнозування.

Ця технологія може дати державним органам нові інструменти, які дозволять скоротити обсяги шахрайства, число помилок і зменшити витрати на паперовий документообіг; великий потенціал для створення нових способів забезпечення прав власності і підтвердження походження товарів та інтелектуальної власності.

Технологія впливає на розробку і створення сервісів для продажу певних послуг, створюються спеціалізовані блокчеїн-консорціуми, які допомагають у вивченні технології та впровадженні її в крипто-індустрію.

На основі впровадження блокчеїн-технології очікується поява нових бізнес-сценаріїв, здатних трансформувати цілі галузі – починаючи з фінансів і закінчуючи охороною здоров'я. Блокчеїн може істотно підвищити податкову дисципліну. Блокчеїн торкається питань розвитку технології, операційної діяльності та трудових ресурсів. Він піднімає нові податкові, юридичні та нормативно-правові питання. Технологія блокчеїн становить загрозу для бізнесу спеціалізованого ПЗ.

Вона може прискорити розвиток розподілених хмарних систем, економіки спільного використання та Інтернет.

Застосування блокчеїн знизить витрати компанії на підготовку звітності, підвищивши її прозорість. Багато галузей вже мають пілотні проекти, які здатні скоротити витрати бізнес-процесів і підвищити ефективність транзакцій. Блокчеїн технологія генерує абсолютно нові бізнес-сценарії, які в майбутньому не тільки повністю перетворять цілі галузі, а й призведуть до зникнення деяких, наприклад, таких як посередництво. Радикальні зміни охоплять бізнес-моделі і процеси, ланцюжки поставок і відносини компаній з клієнтами у всіх секторах економіки.

Технологія блокчеїн відкриває величезний спектр можливостей, починаючи з грошових переказів і платежів і закінчуючи смарт-контрактами і зберіганням документів. Її сильні сторони, такі як зниження витрат, підвищення рівня безпеки та прозорість транзакцій, привернули до себе увагу банківського сектора. Але далеко не всі операції, які до появи технології розподіленої бази даних здійснювалися за допомогою посередників і третіх осіб, можна спростити за допомогою блокчейн. У технології є ряд тонкощів,

пов'язаних і з недостатньою вивченістю, і з розумінням технічної реалізації, і з гнучкістю. Тому ще рано говорити про повну зміну нинішнього вигляду банків під її впливом. Але безперечним є факт про те, що блокчейн здатний перетворити їх внутрішню структуру. Однак для того, щоб технологія розподілених баз даних набула широкого поширення в банківській сфері, необхідно вирішити питання, що стосуються правової легітимності, регулювання, технічної життєздатності, а також стандартизації та широкого впровадження технології.